I855552

(19)中華民國智慧財產局

(12)發明說明書公告本　**(11)證書號數：TW I855552 B**

(45)公告日： 中華民國 113 (2024) 年 09 月 11 日

(21)申請案號：112105515　(22)申請日： 中華民國 112 (2023) 年 02 月 16 日

(51)Int. Cl.：　***G06F21/57 (2013.01)***　***G06F21/60 (2013.01)***

G06F21/62 (2013.01)　*H04L9/14 (2006.01)*

(30)優先權：2022/02/28　世界智慧財產權組織　PCT/JP2022/008320

(71)申請人：日商樂天集團股份有限公司 (日本) RAKUTEN GROUP, INC.　(JP)

日本

(72)發明人：蔡永男 CHAE, YEONGNAM (KR)

(74)代理人：陳長文

(56)參考文獻：

TW	201710941A	TW	201835811A
JP	2006-238273A	JP	2007-156785A
JP	2017-531967A	US	2020/0213111A1
US	2020/0228311A1		

審查人員：施易昉

申請專利範圍項數：18 項　圖式數：12　共 78 頁

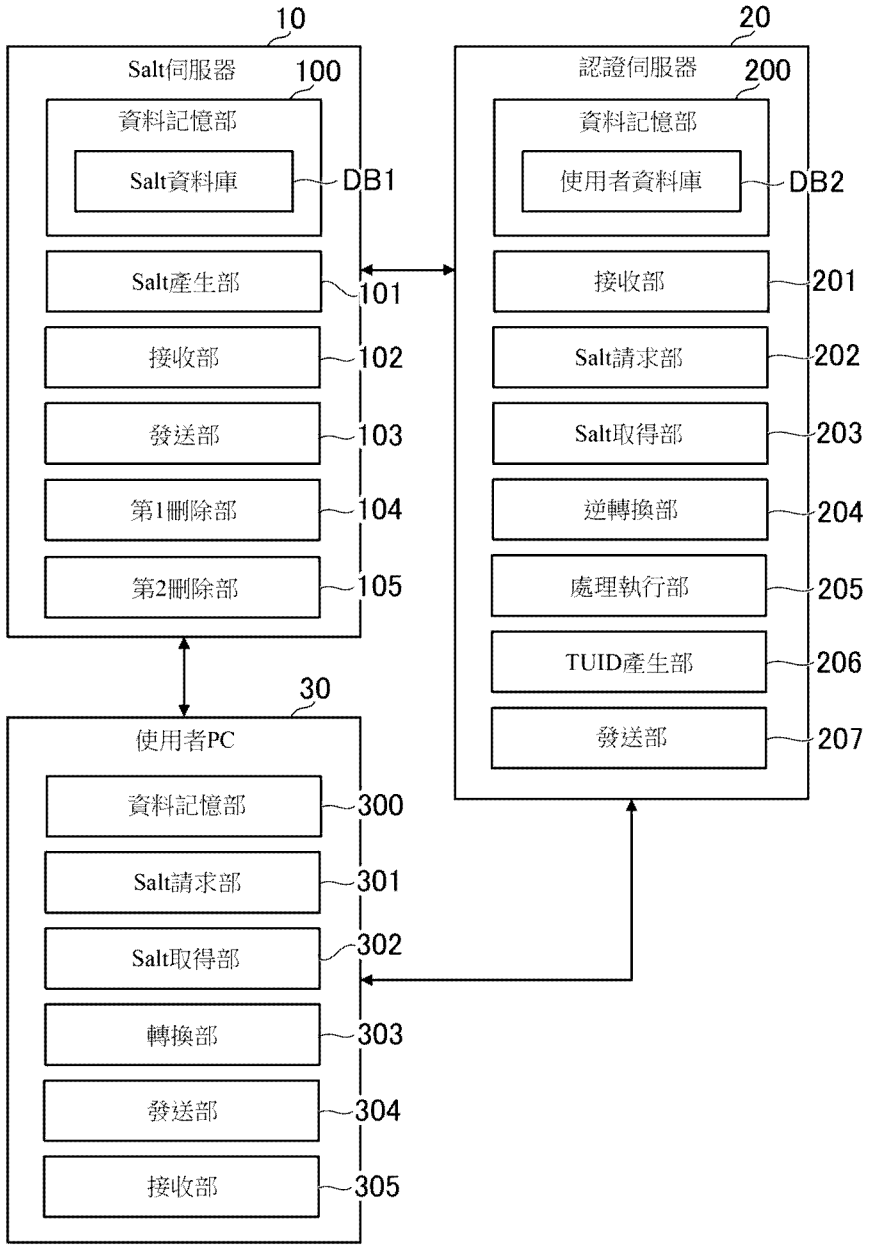
(54)名稱

通信系統、通信方法及程式產品

(57)摘要

本發明之通信系統(S)包含第 1 裝置(30)及第 2 裝置(20)。產生部(101)基於來自第 1 裝置(30)之請求，產生複數個資訊。第 1 裝置(30)基於複數個資訊，轉換原資料並對第 2 裝置(20)發送轉換資料。第 2 裝置(20)基於複數個資訊，將轉換資料進行逆轉換取得原資料。

指定代表圖：



【圖3】

符號簡單說明：

10:Salt 伺服器

20:認證伺服器

30:使用者 PC

100:資料記憶部

101:Salt 產生部

102:接收部

103:發送部

104:第 1 刪除部

105:第 2 刪除部

200:資料記憶部

201:接收部

202:Salt 請求部

203:Salt 取得部

204:逆轉換部

205:處理執行部

206:TUID 產生部

207:發送部

300:資料記憶部

301:Salt 請求部

302:Salt 取得部

303:轉換部

304:發送部

305:接收部

DB1:Salt 資料庫

DB2:使用者資料庫

公告本

I855552

【發明摘要】

【中文發明名稱】

通信系統、通信方法及程式產品

【中文】

本發明之通信系統(S)包含第1裝置(30)及第2裝置(20)。產生部(101)基於來自第1裝置(30)之請求，產生複數個資訊。第1裝置(30)基於複數個資訊，轉換原資料並對第2裝置(20)發送轉換資料。第2裝置(20)基於複數個資訊，將轉換資料進行逆轉換取得原資料。

【指定代表圖】

圖3

【代表圖之符號簡單說明】

10:Salt伺服器

20:認證伺服器

30:使用者PC

100:資料記憶部

101:Salt產生部

102:接收部

103:發送部

104:第1刪除部

105:第2刪除部

200:資料記憶部

201:接收部

202:Salt請求部

203:Salt取得部

204:逆轉換部

205:處理執行部

206:TUID產生部

207:發送部

300:資料記憶部

301:Salt請求部

302:Salt取得部

303:轉換部

304:發送部

305:接收部

DB1:Salt資料庫

DB2:使用者資料庫

【發明說明書】

【中文發明名稱】

通信系統、通信方法及程式產品

【技術領域】

【0001】

本揭示係關於一種通信系統、通信方法及程式產品。

【先前技術】

【0002】

先前，已知有於通信領域，以原資料之內容不被第三者知曉之方式，轉換原資料之技術。例如於專利文獻1，記載有一種技術：基於使用者輸入之使用者ID，產生使用者參數，基於該產生之使用者參數，轉換原資料之一例即生物體資料。例如於專利文獻2，記載有一種技術：利用公開鍵加密方式，轉換原資料之一例即Salt。例如於專利文獻3，記載有一種稱為公開鍵加密方式之一種即挑戰與響應之技術。

[先前技術文獻]

[專利文獻]

【0003】

[專利文獻1]日本專利第4966765號公報

[專利文獻2]日本專利第6866803號公報

[專利文獻3]日本專利再公表2020-85141號公報

【發明內容】

[發明所欲解決之問題]

【0004】

然而，於專利文獻1之技術中，因於網路上發送使用者參數，故有惡意之第三者可容易取得使用者參數。第三者若以某種形式獲取使用者之生物體資料，則可冒充利用非法獲取之使用者參數及生物體資料。因使用者參數基於若一經發行則原則上不變之使用者ID產生，故第三者可利用一經獲取之使用者參數，長期冒充。

【0005】

專利文獻2-3之公開鍵加密方式係利用對第三者公開之公開鍵、與不對第三者公開之秘密鍵之對之加密方式。然而，因秘密鍵為原則上不變之資訊，故若第三者以某種形式獲取秘密鍵，則第三者可利用一經獲取之秘密鍵，長期進行非法行為。於專利文獻1-3之技術中，因可長期進行非法行為，故無法充分提高通信之安全性。

【0006】

本揭示之目的之一在於提高通信之安全性。

[解決問題之技術手段]

【0007】

本揭示之一態樣之通信系統係包含第1裝置及第2裝置者，且包含基於來自上述第1裝置之請求產生複數個資訊之產生部，上述第1裝置基於上述複數個資訊，轉換原資料並對上述第2裝置發送轉換資料，上述第2裝置基於上述複數個資訊，逆轉換上述轉換資料取得上述原資料。

[發明之效果]

【0008】

根據本揭示，通信之安全性提高。

【圖式簡單說明】

【0009】

圖1係顯示通信系統之整體構成之一例之圖。

圖2係顯示第1實施形態之多要素認證之流程之一例之圖。

圖3係顯示由第1實施形態之通信系統實現之功能之一例之功能方塊圖。

圖4係顯示Salt資料庫之一例之圖。

圖5係顯示使用者資料庫之一例之圖。

圖6係顯示由第1實施形態之通信系統執行之處理之一例之圖。

圖7係顯示由第1實施形態之通信系統執行之處理之一例之圖。

圖8係顯示第2實施形態之多要素認證之流程之一例之圖。

圖9係顯示由第2實施形態之通信系統實現之功能區塊之一例之圖。

圖10係顯示第3實施形態之認證系統之整體構成之一例之圖。

圖11係顯示第3實施形態之多要素認證之流程之一例之圖。

圖12係顯示由第3實施形態之認證系統實現之功能區塊之一例之圖。

【實施方式】

【0010】

[1.第1實施形態]

說明本揭示之通信系統之實施形態之例即第1實施形態。於第1實施形態中，列舉於進行使用者之認證之場景應用通信系統之情形為例，但通信系統可應用於任意之場景。對其他場景之應用例由稍後敘述之變化例5說明。

【0011】

[1-1.通信系統之整體構成]

圖1係顯示通信系統之整體構成之一例之圖。如圖1所示，通信系統S包含Salt伺服器10、認證伺服器20、及使用者PC(Personal Computer：個人電腦)30。Salt伺服器10、認證伺服器20、及使用者PC30可連接於網際網路或LAN(Local Area Network：區域網路)等之網路N。通信系統S只要包含至少1台電腦即可，不限於圖1之例。

【0012】

Salt伺服器10為伺服器電腦。控制部11包含至少1個處理器。記憶部12包含RAM(Random Access Memory：隨機存取記憶體)等之揮發性記憶體、與硬碟等之非揮發性記憶體。通信部13包含有線通信用之通信介面、與無線通信用之通信介面中之至少一者。

【0013】

Salt伺服器10為管理裝置之一例。因此，記載為Salt伺服器10之處可換讀為管理裝置。管理裝置可為任意之裝置，不限於Salt伺服器10般之伺服器電腦。例如，管理裝置亦可為個人電腦、平板終端、或智慧型手機。

【0014】

Salt伺服器10管理加密邏輯之Salt。Salt為用於轉換成為轉換對象之資訊之資訊。Salt為與成為轉換對象之資訊一起輸入至轉換函數之資訊。轉換有時亦稱為加密化或哈希化。轉換具有可逆性。轉換後之資訊進行逆轉換，藉此可返回至轉換前之資訊。管理Salt係記憶Salt。

【0015】

Salt自身可利用周知之Salt。例如，Salt為隨機之值。Salt可為任意之形式，例如數字、文字、其他記號、或該等之組合。Salt伺服器10可產生Salt，Salt之產生自身亦可由Salt伺服器10以外之其他裝置進行。

【0016】

認證伺服器20為伺服器電腦。控制部21、記憶部22、及通信部23之物理之構成亦可分別與控制部11、記憶部12、及通信部13同樣。

【0017】

認證伺服器20為第2裝置之一例。因此，記載為認證伺服器20之處可換讀為第2裝置。第2裝置可為任意之裝置，不限於認證伺服器20般之伺服器電腦。例如，第2裝置亦可為個人電腦、平板終端、或智慧型手機。

【0018】

使用者PC30為使用者之個人電腦。控制部31、記憶部32、及通信部33之物理之構成可分別與控制部11、記憶部12、及通信部13同樣。操作部34為滑鼠、鍵盤、或觸控面板等之輸入器件。顯示部35為液晶顯示器或有機EL(Electro Luminescence：電致發光)顯示器。攝影部36包含至少1台相機。

【0019】

使用者PC30為第1裝置之一例。因此，記載為使用者PC30之處可換讀為第1裝置。第1裝置可為任意之裝置，不限於使用者PC30般之個人電腦。例如，第1裝置可為平板終端、智慧型手機、或穿戴式終端。此外例如，第1裝置亦可為遊戲機、自動販賣機、POS(Point Of Sale：銷售點)終端、或ATM(Automatic Teller Machine：自動取款機)之其他裝置。

【0020】

另，記憶於記憶部12、22、32之程式可經由網路N供給。例如，亦可經由讀取電腦可讀取之資訊記憶媒體之讀取部(例如，光碟驅動器或記憶卡槽)、與用於與外部機器進行資料之輸入輸出之輸入輸出部(例如

USB(Universal Serial Bus：通用串列匯流排)埠)中之至少一者，供給記憶於資訊記憶媒體之程式。

【0021】

[1-2.第1實施形態之通信系統之概要]

例如，於通信系統S中，為確認使用者之正當性，而執行多要素認證。多要素認證係組合複數個要素之認證。於第1實施形態中，列舉組合2個要素之2要素認證為例，但亦可為組合3個以上之要素之多要素認證。要素自身可利用各種種類，例如亦可為生物體要素、持有要素、或知識要素。

【0022】

於多要素認證中，利用與要素對應之認證資料。認證資料自身可利用各種種類。例如，於生物體認證中，臉部照片、臉部之特徵量、指紋之照片、指紋之特徵量、靜脈之掃描圖像、或靜脈之特徵量之生物體資料相當於認證資料。於持有認證中，一次性密碼、IC(Integrated Circuit：積體電路)卡所記錄之資訊、或表徵所記錄之資訊之持有資訊相當於認證資料。於知識認證中，使用者ID、密碼、PIN(Personal Identification Number：個人識別號碼)、或秘密之質問之知識資訊相當於認證資料。

【0023】

於第1實施形態中，列舉為登錄至線上服務而執行多要素認證之情形為例，但多要素認證可應用於任意之場景。例如，於申請線上服務時、執行電子結算時、或於線上進行行政手續時之其他場景，亦可應用多要素認證。線上服務自身可應用各種服務。例如，金融服務、通信服務、結算服務、電子商務服務、或SNS(Social Networking Service：社交網路服務)

亦可相當於線上服務。

【0024】

例如，若使用者進行線上服務之利用登錄，則發行用於登錄至線上服務之使用者ID及密碼。使用者以使用者PC30訪問線上服務之網站，輸入使用者ID及密碼。認證伺服器20基於使用者輸入之使用者ID及密碼，確認使用者之正當性。若確認使用者之正當性，則使用者可登錄至線上服務。

【0025】

若每次登錄時請求使用者ID及密碼之輸入，則非常耗費工夫。因此，考慮藉由組合臉部認證及密碼認證之多要素認證，減輕輸入使用者ID之工夫。然而，於該情形時亦產生輸入密碼之工夫。若不產生對操作部34之輸入僅由臉部認證使使用者登錄，則有產生與臉部相似之其他使用者之錯誤認證之可能性。若為包含3D(Dimensional：維)感測器之攝影部36，則可由某種程度之精度執行臉部認證，但即使如此有時亦產生錯誤認證。於攝影部36不包含3D感測器之情形時，錯誤認證之概率提高。亦有以某種形式獲取使用者之臉部照片之第三者冒充使用者之可能性。

【0026】

因此，於第1實施形態中，若為不產生來自操作部34之輸入，且擔保安全性，而使用者登錄至線上服務，則認證伺服器20發行暫時之使用者ID。之後，將該暫時之使用者ID稱為TUID(Temporary User ID：臨時使用者ID)。TUID為可識別使用者之資訊。TUID於滿足特定之無效條件時無效。於第1實施形態中，列舉使用者登錄至線上服務相當於無效條件之情形為例，但無效條件可為任意之條件。例如，無效條件亦可為經過特定

之有效期限、產生一定次數之登錄、或使用者進行特定之操作。

【0027】

認證伺服器20發行之TUID記錄於使用者PC30。於第1實施形態中，雖說明記錄TUID作為瀏覽器之訊錄(cookie)之情形，但亦可記錄TUID作為訊錄以外之資訊。TUID雖亦可顯示於顯示部35，但原則上設為使用者之目光無法觸及者。於第2次以後之登錄中，與臉部認證一起執行利用TUID之TUID認證。因若非為記錄TUID後之使用者PC30則TUID認證不成功，故TUID認證為持有認證之一種。認為若為組合臉部認證及TUID認證之多要素認證，則不產生來自操作部34之輸入，且可擔保某種程度之安全性。

【0028】

然而，若長期重複使用相同之TUID，則有可能被有惡意之第三者盜取有效之TUID。例如，有可能因重放攻擊而被第三者盜取訊錄，亦盜取訊錄所包含之TUID。若第三者除TUID外，亦以某種形式獲取使用者之臉部照片，則可進行冒充。因此，亦考慮於某一定期間使TUID無效。

【0029】

然而，因若TUID即刻無效，則不頻繁登錄之使用者需每次輸入使用者ID及密碼，故使用者之便利性下降。因此，於第1實施形態中，為提高使用者之便利性，且使第三者無法盜取TUID，而利用Salt轉換TUID。但，若長期重複使用相同之Salt，則因有可能被第三者盜取Salt自身，故於使用者每次登錄時產生複數個Salt。

【0030】

圖2係顯示第1實施形態之多要素認證之流程之一例之圖。如圖2所

示，於使用者登錄至線上服務之情形時，使用者PC30對Salt伺服器10發送用於取得Salt之Salt請求。於圖2之例中，createSaltPair()之類之指令包含於Salt請求。因該指令不包含Salt相關之條件，故即使有惡意之第三者窺見Salt請求，亦無法特定於哪種條件下產生Salt。

【0031】

Salt伺服器10若接收Salt請求，則產生Salt之對即第1Salt「6437」及第2Salt「8414」並將其等存儲於Salt資料庫DB1。Salt之對並非當場動態產生，而亦可於Salt資料庫DB1預先存儲多個Salt，Salt伺服器10自Salt資料庫DB1之中取得Salt之對。第1Salt及第2Salt亦可於一定時間自動刪除。Salt伺服器10將第1Salt「6437」及第2Salt「8414」發送至使用者PC30。

【0032】

使用者PC30若自Salt伺服器10接收第1Salt「6437」及第2Salt「8414」，則基於第2Salt「8414」、與特定之轉換函數f，轉換TUID「312456」。於圖2之例中，轉換函數f係對TUID「312456」加上第2Salt「8414」之函數。轉換後之TUID成為該等之和之「320870」。使用者PC30將包含攝影部36產生之使用者之臉部照片、第1Salt「6437」、及轉換後之TUID「320870」之認證請求發送至認證伺服器20。

【0033】

認證伺服器20若接收認證請求，則對Salt伺服器10發送包含第1Salt「6437」之Salt請求。該Salt請求與使用者PC30發送之Salt請求不同。該Salt請求包含getSaltAndDelete(6437)之類之指令。該指令係請求第2Salt「8414」之取得、與第1Salt「6437」及第2Salt「8414」之刪除之指令。

【0034】

Salt伺服器10若接收Salt請求，則參照Salt資料庫DB1，取得與Salt請求所包含之第1Salt「6437」建立關聯之第2Salt「8414」，並發送至認證伺服器20。第1Salt「6437」作為用於檢索第2Salt「8414」之查詢與索引利用。Salt伺服器10自Salt資料庫DB1刪除第1Salt「6437」及第2Salt「8414」。

【0035】

認證伺服器20若自Salt伺服器10接收第2Salt「8414」，則基於該Salt「8414」、與逆轉換函數f^{-1}，將自使用者PC30接收到之轉換後之TUID「320870」進行逆轉換。於圖2之例中，逆轉換函數f^{-1}係自轉換後之TUID「320870」減去第2Salt「8414」之函數。認證伺服器20藉由逆轉換，取得TUID「312456」。

【0036】

認證伺服器20若取得TUID「312456」，則確認於使用者資料庫DB2是否存在TUID「312456」。於使用者資料庫DB2，存儲有成為多要素認證之正解之認證資料。確認有無存在TUID「312456」之處理相當於TUID認證。若於使用者資料庫DB2未存儲TUID「312456」，則於該時點成為錯誤，使用者無法登錄。

【0037】

認證伺服器20若確認TUID「312456」存在於使用者資料庫DB2，則取得與TUID「312456」建立關聯並存儲於使用者資料庫DB2之臉部之特徵量。認證伺服器20基於該取得之臉部之特徵量、與由自使用者PC30接收到之臉部照片計算之臉部之特徵量，執行臉部認證。若臉部認證成功，

則認證伺服器20對使用者PC30發送顯示多要素認證成功之認證結果。使用者PC30若接收該認證結果，則成為登錄至線上服務之狀態。

【0038】

另，於使用者登錄之後，若有惡意之第三者藉由跨網站指令碼(XSS：Cross Site Scripting)攻擊等，盜取轉換後之TUID「320870」、與使用者之臉部照片，則有第三者可冒充之虞。因此，認證伺服器20於使用者登錄之情形時，可發行新的TUID，並將其存儲於使用者資料庫DB2。即，認證伺服器20可於使用者每次登錄時，更新TUID。若新的TUID為「417632」，則認證伺服器20只要對使用者PC30發送包含新的TUID「417632」之認證結果即可。藉此，因使用者每次登錄時TUID改變，故即使第三者進行上述般之跨網站指令碼(XSS)攻擊等亦無法使認證成功，可防止冒充。新的TUID「417632」亦可由自Salt伺服器10接收完畢之第2Salt「8414」轉換。於該情形時，認證伺服器20記憶用於轉換新的TUID之轉換函數，使用者PC30記憶用於將轉換後之新的TUID進行逆轉換之逆轉換函數f^{-1}。即使於該逆轉換中，亦可利用自Salt伺服器10接收完畢之第2Salt「8414」。

【0039】

如以上，第1實施形態之通信系統S基於第1Salt及第2Salt，轉換TUID，或將轉換後之TUID進行逆轉換。藉此，因TUID不直接發送至網路N上，故第三者無法簡單獲取TUID。再者，因第1Salt及第2Salt根據來自使用者PC30之請求動態產生，故即使第三者以某種形式取得第1Salt及第2Salt，亦因於該時點有第1Salt及第2Salt失效之可能性，故通信之安全性提高。之後，說明第1實施形態之通信系統S之細節。

【0040】

[1-3.由第1實施形態之通信系統實現之功能]

圖3係顯示由第1實施形態之通信系統S實現之功能之一例之功能方塊圖。

【0041】

[1-3-1.於Salt伺服器中實現之功能]

資料記憶部100主要實現記憶部12。Salt產生部101、接收部102、發送部103、第1刪除部104、及第2刪除部105主要實現控制部11。

【0042】

[資料記憶部]

資料記憶部100記憶管理Salt所需之資料。例如，資料記憶部100記憶Salt資料庫DB1。若用於轉換TUID之轉換資訊、與用於將轉換後之TUID進行逆轉換之逆轉換資訊為由Salt以外之名字稱呼之資訊，則Salt伺服器10只要利用由Salt資料庫DB1以外之名字稱呼之資料庫，管理轉換資訊及逆轉換資訊即可。

【0043】

圖4係顯示Salt資料庫DB1之一例之圖。Salt資料庫DB1係將複數個Salt相互建立關聯並予以存儲之資料庫。例如，於Salt資料庫DB1，存儲第1Salt及第2Salt之對。之後，於不區別第1Salt及第2Salt時，簡單記載為Salt。於藉由Salt產生部101產生3個以上之Salt之情形時，該等3個以上之Salt相互建立關聯並存儲於Salt資料庫DB1。

【0044】

與Salt資料庫DB1相互建立關聯之複數個Salt為Salt產生部101產生之

複數個資訊之一例。再者，第1Salt為第1資訊之一例，第2Salt為第2資訊之一例。因此，就相互建立關聯之複數個Salt進行說明之處可換讀為複數個資訊。就第1Salt進行說明之處可換讀為第1資訊。就第2Salt進行說明之處可換讀為第2資訊。

【0045】

Salt為轉換資訊之一例，且亦為逆轉換資訊之一例。記載為Salt之處可換讀為轉換資訊。記載為Salt之處亦可換讀為逆轉換資訊。轉換資訊為加密邏輯之加密鍵。逆轉換資訊為加密邏輯之解密鍵。於第1實施形態中，因轉換資訊及逆轉換資訊彼此相同，故轉換資訊及逆轉換資訊相當於加密邏輯之共通鍵。轉換資訊及逆轉換資訊可由鍵以外之名字稱呼，例如檔案之加密化所使用之密碼亦可相當於轉換資訊及逆轉換資訊。

【0046】

轉換資訊及逆轉換資訊可彼此不同。例如，可為轉換資訊為加密邏輯之公開鍵，逆轉換資訊為加密邏輯之秘密鍵。相反地，亦可為轉換資訊為加密邏輯之秘密鍵，逆轉換資訊為加密邏輯之公開鍵。於轉換資訊及逆轉換資訊彼此不同之情形時，於Salt資料庫DB1，存儲轉換資訊及逆轉換資訊之兩者。該等兩者中之轉換資訊發送至使用者PC30，逆轉換資訊發送至認證伺服器20。

【0047】

Salt產生部101產生之各個資訊係通信系統S之通信所利用之資訊。該資訊可為轉換資訊本身，亦可為逆轉換資訊本身。再者，該資訊可為為取得轉換資訊而利用之資訊，亦可為為取得逆轉換資訊而利用之資訊。該資訊可為由Salt以外之任意名字稱呼之資訊。例如，該資訊可為加密邏輯

之鍵、或設定於檔案之密碼。此外例如，該資訊亦可由通行碼或口令暗號之其他名字稱呼。

【0048】

於第1實施形態中，說明第1資訊相當於識別資訊，且第2資訊相當於轉換資訊及逆轉換資訊之情形，但第1資訊及第2資訊之作用亦可為相反之關係。即，亦可為第1資訊相當於轉換資訊及逆轉換資訊，第2資訊為識別資訊。識別資訊係可識別其他資訊之資訊。識別資訊亦可稱為其他資訊之檢索用資訊。利用識別資訊作為檢索其他資訊時之索引。

【0049】

Salt產生部101可產生3個以上之資訊。因此，若將Salt產生部101產生之資訊設為n個(n為3以上之整數)，則可存在第1資訊～第n資訊之n個資訊。例如，於轉換資訊及逆轉換資訊為彼此不同之資訊之情形時，Salt產生部101可產生第1資訊、第2資訊、及第3資訊之3個資訊。於該情形時，可為第1資訊相當於識別資訊，第2資訊相當於轉換資訊，第3資訊相當於逆轉換資訊。第1資訊～第3資訊之作用亦可於識別資訊、轉換資訊、及逆轉換資訊之中替換。

【0050】

另，資料記憶部100可記憶Salt資料庫DB1以外之其他任意之資料。例如，資料記憶部100亦可記憶用於產生Salt之演算法。資料記憶部100亦可記憶用於與認證伺服器20及使用者PC30進行Salt之互換之API(Application Programming Interface：應用程式介面)相關之資料。於第1實施形態中，說明因自認證伺服器20及使用者PC30受理彼此不同形式之Salt請求，故認證伺服器20用之API、與使用者PC30用之API不同之情

形，但亦可自認證伺服器20及使用者PC30統一為相同形式之Salt請求，設為於認證伺服器20及使用者PC30共通之API。

【0051】

[Salt產生部]

Salt產生部101基於來自使用者PC30之請求，產生複數個Salt。例如，Salt產生部101產生第1Salt、及用於進行轉換與逆轉換之第2Salt作為複數個Salt。Salt產生部101基於特定之演算法，產生複數個Salt。例如，Salt產生部101以成為彼此不同之值，且隨機之值之方式，產生複數個Salt。產生隨機之值之方法自身可利用周知之各種方法。例如，可為利用Salt產生時之時間戳之方法，亦可為利用時間戳以外之其他資料之方法。

【0052】

Salt產生部101於Salt資料庫DB1，存儲產生之複數個Salt。於第1實施形態中，Salt產生部101產生第1Salt及第2Salt。Salt產生部101將第1Salt及第2Salt相互建立關聯並存儲於Salt資料庫DB1。相互建立關聯係指可自一者檢索另一者。於第1實施形態中，列舉於TUID之轉換、與轉換後之TUID之逆轉換利用相同之Salt之情形為例。

【0053】

[接收部]

接收部102自認證伺服器20及使用者PC30之各者接收Salt請求。Salt請求係為請求Salt而發送之特定形式之資訊。於圖2中，列舉包含createSaltPair()或getSaltAndDelete(第1Salt)之指令之Salt請求為例，但Salt請求只要為顯示請求Salt之資訊即可，不限於圖2之例。

【0054】

於第1實施形態中，說明來自認證伺服器20之Salt請求、與來自使用者PC30之Salt請求為彼此不同之形式之情形，但該等形式亦可彼此相同。Salt請求為轉換資訊之請求之一例，亦為逆轉換資訊之請求之一例。因此，就Salt請求進行說明之處可換讀為轉換資訊之請求或逆轉換資訊之請求。該等請求可由Salt請求以外之任意名字稱呼。

【0055】

[發送部]

發送部103對認證伺服器20，發送與逆轉換資訊相當之第2Salt。例如，發送部103基於來自認證伺服器20之Salt請求，發送與逆轉換資訊相當之第2Salt。發送部103對使用者PC30，發送與識別資訊相當之第1Salt、及與轉換資訊相當之第2Salt。發送部103基於來自使用者PC30之Salt請求，發送第1Salt及第2Salt。

【0056】

另，於圖3中，雖僅顯示1個發送部103，但亦可將對使用者PC30發送Salt、與對認證伺服器20發送Salt，理解為分開之功能捕捉。因此，亦可視為發送部103係包含於受理來自使用者PC30之Salt請求之情形時，對使用者PC30發送Salt之第1發送部103A，及受理來自認證伺服器20之Salt請求之情形時，對認證伺服器20發送Salt之第2發送部103B。於對使用者PC30之Salt發送順序、與對認證伺服器20之Salt發送順序不同之情形時，第1發送部103A只要照著Salt對使用者PC30之Salt發送順序，對使用者PC30發送Salt即可。第2發送部103B只要照著對認證伺服器20之Salt發送順序，對認證伺服器20發送Salt即可。

【0057】

[第1刪除部]

第1刪除部104係於產生複數個Salt之後，特定之刪除時點來臨之情形時，刪除複數個Salt。刪除時點係應刪除複數個Salt之時點。刪除時點係自產生Salt之產生時點起一定時間後之時點。產生時點至刪除時點之期間之長度可為任意之長度，例如亦可為1秒以內、1秒～10秒左右、或其以上。因刪除後之Salt無效，故刪除時點亦可謂使Salt無效之時點。

【0058】

於圖4中雖予以省略，但於Salt資料庫DB1，存儲第1Salt及第2Salt之刪除時點。第1刪除部104利用即時時鐘或GPS(Global Positioning System：全球定位系統)信號等取得當前時日，判定刪除時點是否已來臨。第1刪除部104自Salt資料庫DB1刪除判定為刪除時點已來臨之第1Salt及第2Salt。

【0059】

另，於Salt資料庫DB1，可存儲第1Salt及第2Salt之產生時點，而非第1Salt及第2Salt之刪除時點。於該情形時，第1刪除部104只要計算自產生時點起一定時間後之刪除時點，判定該計算之刪除時點是否已來臨即可。又，產生時點至刪除時點之期間之長度並非於所有第1Salt及第2Salt共通，亦可根據使用者或時間帶等中之任一條件來設定。

【0060】

[第2刪除部]

第2刪除部105基於來自認證伺服器20之請求，刪除複數個Salt。例如，第2刪除部105於受理來自認證伺服器20之Salt請求，對認證伺服器20發送第2Salt之情形時，刪除第1Salt及第2Salt。即，第2刪除部105係即使

係第1Salt及第2Salt之刪除時點來臨之前，亦會於將第2Salt發送至認證伺服器20，無需第1Salt及第2Salt之情形時，自Salt資料庫DB1刪除第1Salt及第2Salt。

【0061】

[1-3-2.於認證伺服器中實現之功能]

認證伺服器20基於複數個Salt，將轉換資料之一例即轉換後之TUID進行逆轉換，取得原資料之一例即TUID。於第1實施形態中，認證伺服器20將轉換後之TUID進行逆轉換取得TUID，基於該取得之TUID，執行使用者相關之認證處理。資料記憶部200主要實現記憶部22。實現接收部201、Salt請求部202、Salt取得部203、逆轉換部204、處理執行部205、TUID產生部206、及發送部207。

【0062】

[資料記憶部]

資料記憶部200記憶與使用者PC30之通信所需之資料。於第1實施形態中，因於通信系統S中執行多要素認證，故資料記憶部200記憶多要素認證所需之資料。例如，資料記憶部200記憶使用者資料庫DB2。

【0063】

圖5係顯示使用者資料庫DB2之一例之圖。使用者資料庫DB2係存儲使用者相關之資訊之資料庫。例如，於使用者資料庫DB2，存儲使用者ID、密碼、姓名、TUID、臉部照片、及臉部之特徵量。存儲於使用者資料庫DB2之資訊可為任意之種類，不限於圖5之例。例如，用於維持與使用者PC30之通訊期之通訊ID、使用者過去之登錄歷史、或使用者之線上服務之利用歷史亦可存儲於使用者資料庫DB2。

【0064】

臉部照片為生物體資料(生物體資訊)之一例。TUID為與生物體資料不同之認證資料(認證資訊)之一例。因此，就臉部照片進行說明之處可換讀為生物體資料。就TUID進行說明之處可換讀為與生物體資料不同之認證資料。生物體資料、及與生物體資料不同之認證資料之組合亦可為任意之組合。該組合係多要素認證之要素之組合。

【0065】

生物體資料為由生物體認證利用之資料。生物體資料自身可為各種資料，例如臉部之特徵量亦可相當於生物體資料。由臉部之特徵量轉換後之被稱為模板之資訊，可相當於生物體資料。於利用臉部認證以外之生物體認證之情形時，只要利用與生物體認證對應之生物體資料即可。其他生物體資料之例如上所述。與生物體資料不同之認證資料為與生物體資料一起由多要素認證利用之資訊。該認證資料為持有資訊或知識資訊。若為3個要素以上之多要素認證，則與生物體資料不同之認證資料亦可存在複數個。

【0066】

另，資料記憶部200可記憶使用者資料庫DB2以外之其他任意之資料。例如，資料記憶部200可記憶逆轉換函數f^{-1}。例如，資料記憶部200亦可記憶產生TUID之算法。

【0067】

[接收部]

接收部201自使用者PC30，接收第1Salt、與轉換後之TUID。轉換後之TUID為轉換資料之一例。因此，就轉換後之TUID進行說明之處可換讀

為轉換資料。轉換資料係對原資料之一例即TUID進行轉換之資料。原資料係成為轉換之對象之資料。原資料係轉換前之資料。原資料相當於加密邏輯之明文。於第1實施形態中，原資料係使用者PC30之使用者相關之認證資料。因原資料為轉換前之資料，故有時亦稱為原始資料。

【0068】

於第1實施形態中，接收部201自使用者PC30，接收轉換後之TUID、與臉部照片。接收臉部照片係指接收拍攝臉部後之圖像之圖像資料。臉部照片可為靜止圖像，亦可為動態圖像所包含之各個訊框。於第1實施形態中，列舉轉換後之TUID、與臉部照片包含於認證請求之情形為例。因此，接收部201藉由自使用者PC30接收認證請求，接收轉換後之TUID、與臉部照片。認證請求係用於執行多要素認證之請求。只要藉由發送特定形式之資訊進行認證請求即可。認證請求可包含其他資訊。例如，於認證請求，亦可包含如使用者PC30之IP(Internet Protocol：網際網路協定)位址般，可識別使用者PC30之資訊。

【0069】

[Salt請求部]

Salt請求部202基於複數個Salt中之一部分Salt，對Salt伺服器10請求剩餘之Salt。一部分Salt係認證伺服器20自使用者PC30接收到之Salt。剩餘之Salt係認證伺服器20未自使用者PC30接收到之Salt。例如，Salt請求部202基於第1Salt，對Salt伺服器10請求第2Salt。Salt請求部202對Salt伺服器10發送包含第1Salt之Salt請求，藉此請求第2Salt。該Salt請求係用於請求與第1Salt建立關聯之第2Salt之請求。

【0070】

[Salt取得部]

Salt取得部203基於複數個Salt中之一部分Salt，取得剩餘之Salt。一部分Salt係取得剩餘之Salt所利用之Salt。剩餘之Salt係作為逆轉換資訊利用之Salt。例如，Salt取得部203基於第1Salt，取得第2Salt。Salt取得部203為逆轉換資訊取得部之一例。因此，就Salt取得部203進行說明之處可換讀為逆轉換資訊取得部。逆轉換資訊取得部取得將Salt設為一例之逆轉換資訊。於逆轉換資訊由Salt以外之名字稱呼之情形時，逆轉換資訊取得部可由與該名字對應之名字稱呼。例如，於逆轉換資訊稱為鍵或密碼之情形時，逆轉換資訊取得部取得鍵或密碼。

【0071】

於第1實施形態中，因Salt伺服器10管理第1Salt及第2Salt，故Salt取得部203自Salt伺服器10，取得與第1Salt建立關聯之第2Salt。第1Salt及第2Salt亦可由認證伺服器20自身管理。於該情形時，資料記憶部200記憶Salt資料庫DB1。再者，於該情形時，作為由Salt伺服器10實現者說明之Salt產生部101、接收部102、發送部103、第1刪除部104、及第2刪除部105藉由認證伺服器20實現。

【0072】

[逆轉換部]

逆轉換部204基於藉由Salt取得部203取得之剩餘之Salt，將轉換資料之一例即轉換後之TUID進行逆轉換，取得原資料及認證資料之一例即TUID。例如，逆轉換部204基於第2Salt，將轉換後之TUID進行逆轉換，取得TUID。逆轉換部204執行與轉換部303之轉換對應之逆轉換。逆轉換為加密邏輯之解密化。用於逆轉換之逆轉換函數f^{-1}記憶於資料記憶部

200。逆轉換部204基於逆轉換資訊之一例即第2Salt，以逆轉換函數f^{-1}將轉換後之TUID進行逆轉換。根據圖2之例，逆轉換部204藉由自轉換後之TUID減去第2Salt，而將轉換後之TUID進行逆轉換取得TUID。

【0073】

另，逆轉換自身可利用各種逆轉換函數f^{-1}，不限於圖2般之減法。例如，可藉由加法、乘法、除法、矩陣轉換、其他計算、或該等之組合，進行逆轉換。於圖2之例中，顯示為簡化說明，而轉換函數f及逆轉換函數f^{-1}分別為簡單之加法及減法之情形，但實際為某種程度上複雜之計算式。再者，逆轉換不限於加密邏輯之解密化，亦可為壓縮之檔案之解壓。於解壓相當於逆轉換之情形時，壓縮相當於轉換。因對檔案進行某種轉換，故壓縮相當於第1實施形態之轉換。因解壓為將壓縮完畢之檔案返回至原來之狀態之處理，故相當於第1實施形態之逆轉換。

【0074】

[處理執行部]

處理執行部205基於藉由逆轉換取得之認證資料，執行使用者相關之認證處理。於第1實施形態中，作為認證處理之一例說明多要素認證，但認證處理亦可為1要素認證。例如，亦可不利用臉部認證，僅執行TUID之認證。處理執行部205只要執行與應用通信系統S之場景對應之處理即可，處理執行部205執行之處理不限於認證處理。於其他場景應用通信系統S之情形之處理由稍後敘述之變化例說明。處理執行部205只要基於藉由逆轉換部204取得之原資料，執行特定之處理即可。

【0075】

例如，處理執行部205基於藉由逆轉換部204逆轉換後之TUID、與接

收部201接收到之臉部照片，執行多要素認證。如先前所述，多要素認證自身可利用各種種類。於第1實施形態中，處理執行部205參照使用者資料庫DB2，取得與藉由逆轉換部204逆轉換後之TUID建立關聯之臉部之特徵量。該臉部之特徵量為成為多要素認證之正解之認證資料。於存儲於使用者資料庫DB2之臉部之特徵量中，僅與藉由逆轉換部204逆轉換後之TUID建立關聯之臉部之特徵量成為比較對象。其他臉部之特徵量不成為比較對象。

【0076】

處理執行部205基於接收部201接收到之臉部照片，計算臉部之特徵量。臉部之特徵量之計算方法自身可利用各種計算方法。例如，可藉由利用對比度過濾器或主成分分析之計算方法，計算臉部之特徵量。臉部之特徵量可由多維矢量、排列、或單一之數值之任意形式表現。臉部認證並非比較臉部之特徵量彼此者，亦可為將2張臉部照片輸入至機械學習模型判定是否類似之類型者。

【0077】

處理執行部205判定自使用者資料庫DB2取得之臉部之特徵量、與自接收部201接收到之臉部照片計算之臉部之特徵量是否類似。例如，於臉部之特徵量由多維矢量表現之情形時，矢量空間上之臉部之特徵量之距離未達閾值相當於特徵量類似。處理執行部205於臉部之特徵量相互類似之情形時，判定為多要素認證成功。處理執行部205於臉部之特徵量不相互類似之情形時，判定為多要素認證失敗。

【0078】

[TUID產生部]

TUID產生部206基於特定之算法，產生TUID。TUID產生部206於使用者PC30中不存在TUID之情形時，於使用者PC30產生新記錄之TUID。TUID產生部206於使用者PC30中存在TUID之狀態下，取代該TUID產生寫入使用者PC30之TUID(更新後之TUID)。

【0079】

例如，TUID產生部206以成為隨機之值之方式，產生TUID。產生隨機之值之方法自身可利用周知之各種方法。例如，可為利用TUID產生時之時間戳之方法，亦可為利用時間戳以外之其他資料之方法。TUID產生部206於使用者資料庫DB2，存儲產生之TUID。

【0080】

TUID產生部206可以不與其他使用者之TUID重複之方式，產生TUID。TUID產生部206雖允許與臉部不類似之其他使用者之TUID之重複，但亦可以不與臉部類似之其他使用者之TUID重複之方式，產生TUID。TUID產生部206亦可於多要素認證成功之情形時，產生TUID。即，TUID產生部206亦可於使用者每次登錄至線上服務時，產生TUID。若為第1次登錄，則TUID產生部206於使用者ID及密碼之認證成功之情形時，產生TUID。

【0081】

另，產生TUID之時序可為任意之時序，不限於第1實施形態之例。例如，於並非僅1次登錄就使TUID無效，以2次以上之特定次數將相同之TUID設為有效之情形時，TUID產生部206亦可於每次產生該特定次數之登錄時，產生TUID。例如，於TUID設置有效期限之情形時，TUID產生部206亦可於接近有效期限時使用者登錄之情形時，產生TUID。

【0082】

[發送部]

發送部207對使用者PC30，發送多要素認證之認證結果。認證結果為顯示多要素認證是否成功之特定形式之資訊。例如，認證結果顯示是否允許登錄。於第1實施形態中，因於登錄之時序產生新的TUID，故於認證結果，包含新的TUID。

【0083】

另，若多要素認證成功，則允許執行特定之處理。於第1實施形態中，作為該處理之一例，說明對線上服務之登錄，但該處理只要為允許多要素認證成功作為條件之處理即可。該處理只要根據應用通信系統S之場景決定即可。例如，於金融服務應用通信系統S之情形時，轉賬之執行可相當於特定之處理。例如，於結算服務應用通信系統S之情形時，結算之執行可相當於特定之處理。例如，於電子商務服務應用通信系統S之情形時，商品之購入可相當於特定之處理。特定之處理亦可為其他任意之處理。

【0084】

[1-3-3.於使用者PC30中實現之功能]

使用者PC30基於複數個Salt，轉換原資料之一例即TUID，對認證伺服器20發送轉換資料之一例即轉換後之TUID。資料記憶部300主要實現記憶部32。Salt請求部301、Salt取得部302、轉換部303、發送部304、及接收部305主要實現控制部31。

【0085】

[資料記憶部]

資料記憶部300記憶多要素認證所需之資料。例如，資料記憶部300記憶TUID及轉換函數f。於為產生使用者之臉部照片而不利用攝影部36之情形時，資料記憶部300亦可記憶使用者之臉部照片之圖像資料。例如，於準備線上服務用之應用程式之情形時，資料記憶部300亦可記憶該應用程式。

【0086】

[Salt請求部]

Salt請求部301對Salt伺服器10請求複數個Salt。例如，Salt請求部301對Salt伺服器10請求第1Salt及第2Salt。Salt請求部301對Salt伺服器10發送Salt請求，藉此請求Salt。於第1實施形態中，Salt請求部301對Salt伺服器10發送不包含第1Salt及第2Salt之取得規則相關之資訊之Salt請求。例如，於取得基於時間戳產生之第1Salt及第2Salt之情形時，取得規則成為時間戳。因於Salt請求，不包含時間戳之資訊，故不包含取得規則相關之資訊。

【0087】

另，於Salt請求，可包含第1Salt及第2Salt之取得規則。例如，成為用於產生第1Salt及第2Salt之種類之資訊亦可包含於Salt請求。

【0088】

於第1實施形態中，Salt請求部301於藉由攝影部36產生臉部照片之情形時，對Salt伺服器10發送Salt請求。Salt請求部301只要於任意之時序發送Salt請求即可，不限於產生臉部照片之時序。例如，Salt請求部301亦可於線上服務用之應用程式啟動之時序、使用者進行用於登錄之操作之時序、或產生對線上服務之網站之訪問之時序，發送Salt請求。

【0089】

[Salt取得部]

Salt取得部302取得複數個Salt。例如，Salt取得部302取得第1Salt及第2Salt。Salt取得部302於Salt資料庫DB1中，取得相互建立關聯之第1Salt及第2Salt。Salt取得部302為轉換資訊取得部之一例。因此，就Salt取得部302進行說明之處可換讀為轉換資訊取得部。轉換資訊取得部取得將Salt設為一例之轉換資訊。於轉換資訊由Salt以外之名字稱呼之情形時，轉換資訊取得部可由與該名字對應之名字稱呼。例如，於轉換資訊由鍵或密碼稱呼之情形時，轉換資訊取得部取得鍵或密碼。

【0090】

[轉換部]

轉換部303基於複數個Salt中之一部分，轉換原資料及認證資料之一例即TUID。例如，轉換部303基於第2Salt，轉換TUID，產生轉換後之TUID。轉換為加密邏輯之加密化。轉換只要為對TUID進行某種變更者即可。例如，將TUID輸入至某種函數、變更TUID之一部分、變更TUID之全部、對TUID附加某種資訊、或刪除TUID之一部分相當於轉換。逆轉換只要為該等之逆向之處理(將TUID返回至原狀之處理)即可。如上所述，亦可為檔案之壓縮相當於轉換，檔案之解壓相當於逆轉換。於該情形時，利用第2Salt作為密碼，執行壓縮或解壓。

【0091】

用於轉換之轉換函數f記憶於資料記憶部300者。轉換部303基於轉換資訊之一例即Salt，以轉換函數f將轉換前之TUID進行轉換。根據圖2之例，轉換部303藉由對轉換前之TUID加上第2Salt，而將轉換前之TUID進

行轉換，取得轉換後之TUID。轉換自身可利用各種轉換函數，不限於圖2般之加法。例如，亦可藉由加法、乘法、除法、矩陣轉換、其他計算、或該等之組合，進行轉換。

【0092】

[發送部]

發送部304對認證伺服器20發送複數個Salt中之一部分、與轉換後之TUID。發送部304對認證伺服器20發送第1Salt及轉換後之TUID。例如，發送部304對認證伺服器20發送第1Salt、轉換後之TUID、及臉部照片。於第1實施形態中，列舉第1Salt、轉換後之TUID、及臉部照片包含於認證請求之情形為例。因此，說明發送部304對認證伺服器20發送包含第1Salt、轉換後之TUID、及臉部照片之認證請求之情形，但發送部304亦可不將第1Salt、轉換後之TUID、及臉部照片集中於1個資料發送。發送部304亦可分開發送第1Salt、轉換後之TUID、及臉部照片。另，亦可不直接發送臉部照片，而基於Salt或其他加密鍵轉換。亦可於使用者PC30側計算臉部之特徵量，發送該計算後之臉部之特徵量作為生物體資料。

【0093】

[接收部]

接收部305自認證伺服器20接收認證結果。於該認證結果顯示成功之情形時，使用者登錄至線上服務。即，允許執行上述特定之處理。於新的TUID包含於認證結果之情形時，接收部305將認證結果所包含之TUID記錄於資料記憶部300。自資料記憶部300廢棄至此為止記錄之舊的TUID。

【0094】

[1-4.由第1實施形態之通信系統執行之處理]

圖6及圖7係顯示由第1實施形態之通信系統S執行之處理之一例之圖。藉由控制部11、21、31分別執行記憶於記憶部12、22、32之程式，而執行圖6及圖7之處理。於執行圖6及圖7之處理時，使用者之使用者ID及密碼發行完畢。

【0095】

如圖6所示，使用者PC30使線上服務之應用程式啟動，判定於記憶部32是否有TUID(S1)。於判定為無TUID之情形時(S1；N)，使用者PC30基於操作部34之檢測信號，受理使用者之使用者ID及密碼之輸入(S2)。於認證伺服器20及使用者PC30之間，執行用於登錄至線上服務之登錄處理(S3)。於S3中，基於使用者資料庫DB2，確認使用者ID及密碼之正當性。若登錄成功，則認證伺服器20發行新的TUID(S4)，對使用者PC30發送包含新的TUID之認證結果(S5)。

【0096】

使用者PC30若接收認證結果(S6)，則將認證結果所包含之TUID記錄於記憶部32(S7)，本處理結束。於S7中，TUID亦可作為訊錄之一部分記錄。之後，使用者PC30執行用於使使用者利用線上服務之處理。若使用者進行用於自線上服務登出之操作，則於認證伺服器20及使用者PC30之間，執行用於自線上服務登出之登錄處理。

【0097】

於S1中，判定為有TUID之情形時(S1；是(Y))，使用者PC30基於攝影部36，拍攝使用者之臉部產生臉部照片(S8)。使用者PC30對Salt伺服器10發送Salt請求(S9)。Salt伺服器10若接收Salt請求(S10)，則產生第1Salt及第2Salt並存儲於Salt資料庫DB1，對使用者PC30發送該第1Salt及第

2Salt(S11)。使用者PC30若自Salt伺服器10接收第1Salt及第2Salt(S12)，則基於第2Salt，轉換記憶部32所記憶之TUID(S13)。

【0098】

移行至圖7，使用者PC30對認證伺服器20發送包含S12中接收到之第1Salt、S13之轉換後之TUID、及S8中產生之臉部照片之認證請求(S14)。認證伺服器20若接收認證請求(S15)，則對Salt伺服器10發送包含第1Salt之Salt請求(S16)。Salt伺服器10若接收Salt請求(S17)，則基於Salt資料庫DB1，對認證伺服器20發送與第1Salt建立關聯之第2Salt(S18)。

【0099】

認證伺服器20若自Salt伺服器10接收第2Salt(S19)，則基於該第2Salt，將S15中接收到之認證請求所包含之轉換後之TUID進行逆轉換(S20)。認證伺服器20基於S20中逆轉換後之TUID、與S15中接收到之認證請求所包含之臉部照片，執行多要素認證(S21)。於S21中，認證伺服器20基於使用者資料庫DB2，取得與S20中逆轉換後之TUID建立關聯之臉部之特徵量。認證伺服器20基於S15中接收到之臉部照片，計算臉部之特徵量。認證伺服器20判定該取得之臉部之特徵量之類似度是否為閾值以上。於TUID存在於使用者資料庫DB2，臉部之特徵量之類似度為閾值以上之情形時，多要素認證成功。

【0100】

認證伺服器20判定多要素認證是否成功(S22)。於多要素認證失敗之情形時(S22；否(N))，本處理結束。於該情形時，亦可請求使用者ID及密碼之輸入。於多要素認證成功之情形時(S22；是)，允許使用者對線上服務之登錄，移行至S4之處理。藉由S4以後之處理，更新使用者PC30之

TUID。

【0101】

根據第1實施形態之通信系統S，使用者PC30基於複數個Salt，轉換TUID並對認證伺服器20發送轉換後之TUID。認證伺服器20基於複數個Salt，將轉換後之TUID進行逆轉換取得TUID。藉此，將轉換後之TUID發送至網路上，因第三者不易取得TUID，故通信之安全性提高。即使有惡意之第三者自認證伺服器20盜取對Salt伺服器10之Salt請求，亦因僅第1Salt難以把握轉換之組成，故通信之安全性進而提高。再者，因基於自使用者PC30對Salt伺服器10之Salt請求產生第1Salt及第2Salt，故即使第三者以某種形式盜取第1Salt及第2Salt，於該時點第1Salt及第2Salt成為無效之可能性亦較高，可防止第三者之非法行為。

【0102】

又，使用者PC30對認證伺服器20，發送基於第1Salt、與第2Salt轉換之轉換後之TUID。認證伺服器20基於第1Salt，取得第2Salt，基於該取得之第2Salt，將轉換後之TUID進行逆轉換取得TUID。藉此，利用2個Salt之對提高通信之安全性。藉由利用第2Salt作為轉換資訊及逆轉換資訊之兩者，而藉由更少之Salt可擔保安全性。因此，可將用於提高通信之安全性之處理簡化，並減輕通信系統S整體之處理負荷。

【0103】

又，Salt伺服器10基於來自使用者PC30之Salt請求，產生第1Salt及第2Salt。Salt伺服器10基於來自認證伺服器20之Salt請求，對認證伺服器20發送第2Salt。藉此，因認證伺服器20不必管理第1Salt及第2Salt，故可分散通信之處理負荷。即，可由Salt伺服器10及認證伺服器20分散處理。

因此，可減輕認證伺服器20之處理負荷。

【0104】

又，使用者PC30對Salt伺服器10，發送不包含第1Salt及第2Salt之取得規則相關之資訊之Salt請求。藉此，即使有惡意之第三者盜取Salt請求，亦不易解讀TUID之轉換之組成。例如，即使取得與時間戳對應之第1Salt及第2Salt，亦因僅Salt請求無法把握該取得規則，故通信之安全性進而提高。

【0105】

又，Salt伺服器10係於產生複數個Salt之後，特定之刪除時點來臨之情形時，刪除複數個Salt。藉此，因自Salt資料庫DB1刪除不需要之Salt，可確實地防止Salt流出，故通信之安全性進而提高。亦可抑制Salt資料庫DB1之記憶體消耗量。

【0106】

又，Salt伺服器10基於來自認證伺服器20之請求，刪除複數個Salt。藉此，因自Salt資料庫DB1刪除不需要之Salt，可確實地防止Salt流出，故通信之安全性進而提高。亦可抑制Salt資料庫DB1之記憶體消耗量。

【0107】

又，認證伺服器20將轉換後之TUID進行逆轉換取得TUID，基於該取得之TUID，執行使用者相關之認證處理，於認證處理成功之情形時，產生新的TUID。藉此，認證時之安全性提高。例如，因於使用者每次登錄時TUID改變，故即使第三者進行先前所述之跨網站指令碼攻擊等亦無法使認證成功，因此可防止冒充。

【0108】

[2.第2實施形態]

於第1實施形態中，對藉由於Salt之取得方法上耗費工夫，提高通信之安全性之情形進行說明。提高通信之安全性之方法不限於第1實施形態之例。於第2實施形態中，根據第1Salt區分使用轉換函數f，藉此提高通信之安全性。於以後之第2實施形態及第3實施形態中，對與第1實施形態同樣之點省略說明。

【0109】

圖8係顯示第2實施形態之多要素認證之流程之一例之圖。於第2實施形態中，大致之流程可與第1實施形態同樣。於圖8之例中，第1Salt及第2Salt之取得方法與第1實施形態同樣。與第1實施形態之圖2之例同樣，使用者PC30自Salt伺服器10取得第1Salt「6437」及第2Salt「8414」。

【0110】

於第2實施形態中，使用者PC30基於第1Salt「6437」之後1碼，區分使用轉換函數f。例如，使用者PC30記憶與後1碼「0」～「9」分別對應之轉換函數f0～f9。之後，於不區別轉換函數f0～f9時，簡單記載為轉換函數f。各個轉換函數f所示之計算方法彼此不同。因此，若即使為相同之Salt轉換函數f亦不同，則轉換後之TUID之值亦不同。

【0111】

於圖8之例中，選擇與第1Salt「6437」之後1碼「7」對應之轉換函數f7。該轉換函數f7與第1實施形態之圖2所說明之轉換函數f同樣。選擇轉換函數f7之後之使用者PC30之處理與第1實施形態同樣。認證伺服器20若接收第1Salt「6437」及轉換完畢之TUID「320870」，則與第1實施形態同樣，自Salt伺服器10取得第1Salt「6437」。

【0112】

於第2實施形態中，認證伺服器20基於第1Salt「6437」之後1碼「7」，區分使用逆轉換函數f^{-1}。例如，認證伺服器20記憶與後1碼「0」～「9」分別對應之逆轉換函數$f^{-1}0$～$f^{-1}9$。之後，於不區別逆轉換函數$f^{-1}0$～$f^{-1}9$時，簡單記載為逆轉換函數f^{-1}。各個逆轉換函數f^{-1}所示之計算方法彼此不同。因此，若即使為相同之第2Salt「8414」逆轉換函數f^{-1}亦不同，則逆轉換後之TUID之值亦不同。

【0113】

於圖8之例中，選擇與第1Salt「6437」之後1碼「7」對應之逆轉換函數$f^{-1}7$。該逆轉換函數$f^{-1}7$與第1實施形態之圖2所說明之逆轉換函數f^{-1}同樣。包含選擇逆轉換函數$f^{-1}7$之後之認證伺服器20之處理之多要素認證之流程，係與第1實施形態同樣。

【0114】

圖9係顯示由第2實施形態之通信系統S實現之功能區塊之一例之圖。如圖9所示，於第2實施形態中，實現逆轉換函數選擇部208及轉換函數選擇部306。逆轉換函數選擇部208主要實現控制部21。轉換函數選擇部306主要實現控制部31。於第2實施形態中，第1Salt雖為用於取得第2Salt之識別資訊，但亦為用於選擇TUID之轉換方法及逆轉換方法之資訊。

【0115】

轉換函數選擇部306基於第1Salt，選擇複數個轉換函數f中之任一者。轉換函數f為轉換方法之一例。因此，就轉換函數f進行說明之處，可換讀為轉換方法。轉換方法係轉換TUID之方法。轉換方法只要為定義如何轉換TUID者即可，不限於轉換函數f。例如，轉換方法可為不稱為函數

之計算式、或加密化演算法。此外例如，轉換方法亦可為檔案壓縮之演算法。

【0116】

轉換函數選擇部306只要基於第1Salt相關之特定之選擇方法，選擇複數個轉換函數f中之任一者即可。該選擇方法係轉換函數f之選擇方法。該選擇方法係第1Salt成為條件之方法。若第1Salt之值改變，則選擇之轉換函數f亦可改變。例如，轉換函數選擇部306基於第1Salt之一部分，選擇複數個轉換函數f中之任一者。轉換函數選擇部306亦可基於第1Salt之全部，選擇轉換函數f。

【0117】

於第2實施形態中，說明利用第1Salt之後1碼之值作為選擇方法之一例之情形。轉換函數選擇部306選擇與第1Salt之後1碼對應之轉換函數f。將第1Salt之後1碼及轉換函數f之關係，預先定義於資料記憶部300。轉換函數選擇部306選擇與第1Salt之後1碼對應之轉換函數f。於第2實施形態中，第1Salt之後1碼可取得之數值「0」～「9」、與轉換函數「f0」～「f9」所包含之數值相互對應。

【0118】

於第2實施形態中，轉換函數選擇部306不對其他裝置請求選擇轉換函數f，而基於第1Salt，選擇複數個轉換函數f中之任一者。其他裝置係使用者PC30以外之裝置。例如，其他裝置為Salt伺服器10、認證伺服器20、或其他伺服器電腦。轉換函數選擇部306於取得第1Salt之後，僅以使用者PC30內之處理，使轉換函數f之選擇完成。於稍後敘述之第3實施形態中，與第2實施形態不同，會產生藉由其他裝置來選擇轉換函數f之情

形。

【0119】

轉換部303基於藉由轉換函數選擇部306選擇之轉換函數f，產生轉換後之TUID。利用藉由轉換函數選擇部306選擇之轉換函數f之點係與第1實施形態不同，但其他點同樣。

【0120】

逆轉換函數選擇部208基於第1Salt，選擇複數個逆轉換函數f^{-1}中之任一者。逆轉換函數f^{-1}為逆轉換方法之一例。因此，對逆轉換函數f^{-1}進行說明之處可換讀為逆轉換方法。逆轉換方法係將轉換後之TUID進行逆轉換之方法。逆轉換方法只要為定義如何將轉換後之TUID進行逆轉換者即可，不限於逆轉換函數f^{-1}。例如，逆轉換方法可為不稱為函數之計算式、或解密化演算法。此外例如，逆轉換方法亦可為檔案解壓之演算法。

【0121】

逆轉換函數選擇部208基於第1Salt相關之特定之選擇方法，選擇複數個逆轉換函數f^{-1}中之任一者。該選擇方法係逆轉換函數f^{-1}之選擇方法。該選擇方法係第1Salt成為條件之方法。若第1Salt之值改變，則選擇之逆轉換函數f^{-1}亦可改變。例如，逆轉換函數選擇部208基於第1Salt之一部分，選擇複數個逆轉換函數f^{-1}中之任一者。逆轉換函數選擇部208亦可基於第1Salt之全部，選擇逆轉換函數f^{-1}。

【0122】

於第2實施形態中，說明利用第1Salt之後1碼作為逆轉換函數f^{-1}之選擇方法之一例之情形。逆轉換函數選擇部208選擇與第1Salt之後1碼對應之逆轉換函數f^{-1}。第1Salt之後1碼及逆轉換函數f^{-1}之關係預先定義於資料

記憶部200。逆轉換函數選擇部208選擇與第1Salt之後1碼對應之逆轉換函數f^{-1}。例如，逆轉換函數選擇部208選擇與第1Salt之後1碼對應之逆轉換函數f^{-1}，作為藉由轉換函數選擇部306選擇之轉換函數f所對應之逆轉換函數f^{-1}。

【0123】

於第2實施形態中，逆轉換函數選擇部208不對其他裝置請求逆轉換函數f^{-1}之選擇，而基於第1Salt，選擇複數個逆轉換函數f^{-1}中之任一者。逆轉換函數選擇部208於取得第1Salt之後，僅由認證伺服器20內之處理，使逆轉換函數f^{-1}之選擇完成。於稍後敘述之第3實施形態中，與第2實施形態不同，產生藉由其他裝置之逆轉換函數f^{-1}之選擇。

【0124】

逆轉換部204基於藉由逆轉換函數選擇部208選擇之逆轉換函數f^{-1}，取得TUID。利用藉由逆轉換函數選擇部208選擇之逆轉換函數f^{-1}之點與第1實施形態及第2實施形態不同，但其他點同樣。

【0125】

根據第2實施形態之通信系統S，使用者PC30基於第1Salt，選擇複數個轉換函數f中之任一者。認證伺服器20基於第1Salt，選擇複數個逆轉換函數f^{-1}中之任一者。藉此，因轉換函數f動態改變，故第三者不易把握轉換之組成，通信之安全性進而提高。即使有惡意之第三者盜取Salt請求，亦因以第1Salt難以把握轉換之組成，故通信之安全性進而提高。

【0126】

又，使用者PC30不對其他裝置請求選擇轉換函數f，而基於第1Salt，選擇複數個轉換函數f中之任一者。認證伺服器20不對其他裝置請

求逆轉換函數f-1之選擇，而基於第1Salt，選擇複數個逆轉換函數f-1中之任一者。藉此，為選擇轉換函數f及逆轉換函數f-1，而不產生對其他裝置之請求，故可將通信時之處理簡化。亦可縮短至多要素認證之完成為止所需之時間。

【0127】

又，使用者PC30基於第1Salt之一部分，選擇複數個轉換函數f中之任一者。認證伺服器20基於第1Salt之一部分，選擇複數個逆轉換函數f^{-1}中之任一者。藉此，因並非為取得第2Salt而利用第1Salt，而為選擇轉換函數f及逆轉換函數f^{-1}而可利用第1Salt，故可更有效活用第1Salt。為選擇轉換函數f及逆轉換函數f^{-1}，而無需重新準備第1Salt以外之其他資訊，故可將選擇轉換函數f及逆轉換函數f^{-1}之方法簡化。

【0128】

[3.第3實施形態]

於第2實施形態中，說明認證伺服器20及使用者PC30分別選擇逆轉換函數f^{-1}及轉換函數f之情形，但逆轉換函數f^{-1}及轉換函數f亦可藉由第三者伺服器選擇。

【0129】

圖10係顯示第3實施形態之認證系統S之整體構成之一例之圖。如圖10所示，第3實施形態之認證系統S包含選擇伺服器40。選擇伺服器40為伺服器電腦。控制部41、記憶部42、及通信部43之物理構成可分別與控制部11、記憶部12、及通信部13同樣。選擇伺服器40為選擇裝置之一例。因此，記載為選擇伺服器40之處可換讀為選擇裝置。

【0130】

選擇裝置係選擇轉換函數f及逆轉換函數f^{-1}之裝置。選擇裝置可為任意之裝置，不限於選擇伺服器40般之伺服器電腦。例如，選擇裝置可為個人電腦、平板終端、或智慧型手機。此外例如，選擇裝置亦可為遊戲機、自動販賣機、POS終端、或ATM之其他裝置。

【0131】

圖11係顯示第3實施形態之多要素認證之流程之一例之圖。於第3實施形態中，大致之流程可與第2實施形態同樣。至使用者PC30取得第1Salt及第2Salt之流程與第2實施形態同樣。但，圖11中，將第1Salt設為「6430」。

【0132】

於第3實施形態中，使用者PC30對選擇伺服器40發送第1Salt「6430」。選擇伺服器40記憶函數資料庫DB3。將第1Salt之後1碼、轉換函數f、及逆轉換函數f^{-1}與函數資料庫DB3建立關聯。於圖11之例中，因f之後之數值相同之逆轉換函數f^{-1}對應，故雖於函數資料庫DB3僅顯示轉換函數f，但於函數資料庫，亦可存儲轉換函數f及逆轉換函數f^{-1}之兩者。函數資料庫DB3之關聯於特定之時序更新。例如，選擇伺服器40定期隨機更新函數資料庫DB3之關聯。

【0133】

選擇伺服器40基於自使用者PC30接收到之第1Salt「6430」之後1碼「0」，選擇轉換函數f。選擇轉換函數f之主體成為選擇伺服器40，但轉換函數f之選擇方法自身可與第2實施形態同樣。選擇伺服器40對使用者PC30發送轉換函數f之選擇結果「f7」。使用者PC30若接收轉換函數f之選擇結果「f7」，則轉換TUID「312456」。該轉換自身可與第2實施形態同

樣。之後之流程之認證伺服器20自Salt伺服器10取得第2Salt「8414」為止與第2實施形態同樣。

【0134】

認證伺服器20對選擇伺服器40，發送第1Salt「6430」。選擇伺服器40基於自認證伺服器20接收到之第1Salt「6430」之後1碼「0」，選擇逆轉換函數f^{-1}。選擇逆轉換函數f^{-1}之主體成為選擇伺服器40，但逆轉換函數f^{-1}之選擇方法自身可與第2實施形態同樣。選擇伺服器40對認證伺服器20發送逆轉換函數f^{-1}之選擇結果「$f^{-1}7$」。認證伺服器20若接收逆轉換函數f^{-1}之選擇結果，則將轉換完畢之TUID「320870」進行逆轉換。該逆轉換自身可與第2實施形態同樣。之後之多要素認證之流程與第2實施形態同樣。

【0135】

圖12係顯示由第3實施形態之認證系統S實現之功能區塊之一例之圖。如圖12所示，於第3實施形態中，實現逆轉換函數請求部209、轉換函數請求部307、資料記憶部400、轉換函數選擇部401、逆轉換函數選擇部402、及更新部403。逆轉換函數請求部209主要實現控制部21。轉換函數請求部307主要實現控制部31。資料記憶部400主要實現記憶部42。轉換函數選擇部401、逆轉換函數選擇部402、及更新部403主要實現控制部41。

【0136】

轉換函數請求部307基於第1Salt，對選擇伺服器40請求選擇轉換函數f。之後，將該請求稱為轉換函數選擇請求。轉換函數選擇請求只要藉由特定之形式進行即可。轉換函數選擇請求可包含成為用於選擇伺服器40選擇轉換函數f之基準之資訊，亦可僅包含選擇轉換函數f之主旨之指令。

於第3實施形態中，說明轉換函數選擇請求包含第1Salt之情形，但轉換函數選擇請求亦可僅包含第1Salt之後1碼。

【0137】

逆轉換函數請求部209基於第1Salt，對選擇伺服器40請求逆轉換函數f^{-1}之選擇。之後，將該請求稱為逆轉換函數選擇請求。逆轉換函數選擇請求只要藉由特定之形式進行即可。逆轉換函數選擇請求可包含成為用於選擇伺服器40選擇逆轉換函數f^{-1}之基準之資訊，亦可僅包含選擇逆轉換函數f^{-1}之主旨之指令。於第3實施形態中，說明逆轉換函數選擇請求包含第1Salt之情形，但逆轉換函數選擇請求亦可僅包含第1Salt之後1碼。

【0138】

轉換函數選擇部401基於來自使用者PC30之轉換函數選擇請求，選擇複數個轉換函數f中之任一者。於第3實施形態中，與第2實施形態同樣，說明該選擇方法為第1Salt之後1碼之值之情形，但選擇方法亦可為其他任意之方法。例如，可為第1Salt之前1碼之值，亦可為第2Salt之值。轉換函數選擇部401發送選擇伺服器40選擇之可識別轉換函數f之資訊作為選擇結果。

【0139】

逆轉換函數選擇部402基於來自認證伺服器20之逆轉換函數選擇請求，選擇複數個逆轉換函數f^{-1}中之任一者。於第3實施形態中，與第2實施形態同樣，說明該選擇方法為第1Salt之後1碼之值之情形，但選擇方法亦可為其他任意之方法。例如，可為第1Salt之前1碼之值，亦可為第2Salt之值。逆轉換函數選擇部402發送選擇伺服器40選擇之可識別逆轉換函數f^{-1}之資訊作為選擇結果。

【0140】

轉換函數選擇部306基於選擇伺服器40之選擇結果，選擇轉換函數f。利用藉由選擇伺服器40選擇之轉換函數f之點與第1實施形態及第2實施形態不同，但其他點同樣。

【0141】

逆轉換函數選擇部208基於選擇伺服器40之選擇結果，選擇逆轉換函數f^{-1}。利用藉由選擇伺服器40選擇之逆轉換函數f^{-1}之點與第1實施形態及第2實施形態不同，但其他點同樣。

【0142】

更新部403將第1Salt相關之選擇條件、與複數個轉換函數f及複數個逆轉換函數f^{-1}之各者之關聯更新。於第3實施形態中，因該等關聯存儲於函數資料庫DB3，故更新部403更新函數資料庫DB3。更新部403於滿足特定之更新條件之情形時，更新函數資料庫DB3之關聯。

【0143】

更新條件係用於更新函數資料庫DB3之關聯之條件。更新條件可為任意之條件，例如亦可為時間性條件、或轉換函數f與逆轉換函數f^{-1}之選擇次數相關之條件。例如，管理者進行特定之操作可相當於更新條件。於第3實施形態中，說明更新條件為時間性條件，更新部403於特定之更新時點來臨時，更新關聯之情形。更新時點可為任意之時點，例如可為1日之特定時刻，亦可為1週或1月之中設定之時點。

【0144】

更新部403只要以成為與更新前之關聯不同之關聯之方式，更新函數資料庫DB3即可。例如，更新部403以打亂第1Salt之後1碼之值、與轉換

函數f及逆轉換函數f^{-1}之組合之方式，更新關聯。轉換函數選擇部401於藉由更新部403更新關聯之後，基於更新後之關聯，選擇轉換函數f。逆轉換函數選擇部402於藉由更新部403更新關聯之後，基於更新後之關聯，選擇逆轉換函數f^{-1}。利用更新後之關聯之點雖與選擇上述轉換函數f及逆轉換函數f^{-1}之處理不同，但其他點同樣。

【0145】

根據第3實施形態之認證系統S，選擇伺服器40基於來自認證伺服器20及使用者PC30之請求，選擇逆轉換函數f^{-1}及轉換函數f。藉此，因認證伺服器20及使用者PC30無需持有選擇逆轉換函數f^{-1}及轉換函數f之演算法，故可將多要素認證之組成簡化。再者，因容易定期變更定義於函數資料庫DB3之逆轉換函數f^{-1}及轉換函數f，故第三者不易推測轉換之組成，通信之安全性提高。

【0146】

又，選擇伺服器40將第1Salt相關之選擇條件、與複數個轉換函數f及複數個逆轉換函數f^{-1}之各者之關聯更新。藉此，因逆轉換函數f^{-1}及轉換函數f之選擇方法改變，第三者不易特定逆轉換及轉換之組成，故通信之安全性進而提高。

【0147】

[4.變化例]

另，本揭示並非限定於以上說明之第1實施形態～第3實施形態者。於不脫離本揭示之主旨之範圍內，可進行適當變更。

【0148】

[4-1.變化例1]

例如，於第3實施形態之圖11之例中，將選擇伺服器40受理來自使用者PC30之轉換函數選擇請求之時點，設為快到函數資料庫DB3之更新時點之前。於該情形時，若將選擇伺服器40受理來自認證伺服器20之逆轉換函數選擇請求之時點設為函數資料庫DB3之更新時點緊接之後，則有TUID之轉換所利用之轉換函數f、與轉換後之TUID之逆轉換所利用之逆轉換函數f^{-1}不相互對應之可能性。

【0149】

因此，變化例1中，於快到函數資料庫DB3之更新時點之前，選擇伺服器40受理來自使用者PC30之轉換函數選擇請求之情形時，可將選擇轉換函數f之選擇時點相關之資訊發送至認證伺服器20。發送部304對認證伺服器20，進而發送選擇轉換函數f之選擇時點相關之時點資訊。時點資訊係可識別是否於更新函數資料庫DB3之前選擇轉換函數f之資訊。時點資訊可自選擇伺服器40發送至使用者PC30，亦可於使用者PC30預先把握更新時點之情形時，藉由使用者PC30產生。

【0150】

逆轉換函數選擇部402於更新函數資料庫DB3之關聯緊接之後立即受理來自認證伺服器20之請求之情形時，基於更新前之關聯，選擇第1逆轉換函數f^{-1}，且基於更新後之關聯，選擇第2逆轉換函數f^{-1}。此處之緊接之後意味著時間性長度未達閾值。因此，函數資料庫DB3之關聯之更新時點、與受理來自認證伺服器20之請求選擇轉換函數f之選擇時點之間之時間性長度未達閾值，相當於緊接之後。

【0151】

逆轉換函數選擇部402判定受理來自認證伺服器20之逆轉換函數選擇

請求之時點是否為函數資料庫DB3之更新之後。逆轉換函數選擇部402於判定該時點為函數資料庫DB3之更新之後之情形時，選擇基於更新前之關聯之第1逆轉換函數f^{-1}、與基於更新後之關聯之第2逆轉換函數f^{-1}。於資料記憶部400，亦保持更新前之函數資料庫DB3。

【0152】

逆轉換函數選擇部208基於時點資訊，選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}中之任一者。逆轉換函數選擇部208於時點資訊顯示更新函數資料庫DB3之前選擇了轉換函數f之情形時，選擇第1逆轉換函數f^{-1}。逆轉換函數選擇部208於時點資訊顯示更新函數資料庫DB3之後選擇了轉換函數f之情形時，選擇第2逆轉換函數f^{-1}。

【0153】

根據變化例1，選擇伺服器40於更新函數資料庫DB3之關聯緊接之後立即受理來自認證伺服器20之請求之情形時，基於更新前之關聯，選擇第1逆轉換函數f^{-1}，且基於更新後之關聯，選擇第2逆轉換函數f^{-1}。認證伺服器20基於時點資訊，選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}中之任一者。藉此，即使於更新時點間選擇了轉換函數f，亦可準確執行逆轉換。因此，因可省去多要素認證失敗重新操作之工夫，故使用者之便利性提高。因Salt伺服器10、認證伺服器20、使用者PC30、及選擇伺服器40亦不執行不需要之處理，故可減輕該等之處理負荷。

【0154】

[4-2.變化例2]

例如，認為於藉由選擇伺服器40選擇轉換函數f之選擇時點並非快到更新時點之前之情形時，不產生變化例1般之問題。因此，使用者PC30亦

可於選擇轉換函數f之選擇時點並非快到更新時點之前之情形時，不對認證伺服器20發送時點資訊，於選擇時點為快到更新時點之前之情形時，對認證伺服器20發送時點資訊。此處所謂之快到更新時點之前，意味著時間性長度未達閾值。選擇時點至更新時點之時間性長度未達閾值，相當於快到更新時點之前。

【0155】

選擇時點是否為快到更新時點之前亦可藉由使用者PC30判定，但此處，藉由選擇伺服器40判定。選擇伺服器40預先把握以下之更新時點。選擇伺服器40受理來自使用者PC30之轉換函數選擇請求，判定選擇轉換函數f之選擇時點至更新時點之時間之長度是否未達閾值。將該判定結果通知至使用者PC30。

【0156】

使用者PC30於選擇時點並非快到更新時點之前之情形時，亦可原本不自選擇伺服器40接收時點資訊。使用者PC30即使自選擇伺服器40接收時點資訊，若選擇時點並非快到更新時點之前，則亦不對認證伺服器20發送時點資訊。使用者PC30自選擇伺服器40接收選擇時點是否為快到更新時點之前之判定結果。使用者PC於選擇時點為快到更新時點之前之情形時，與變化例1同樣，對認證伺服器20發送時點資訊。

【0157】

逆轉換函數選擇部402於選擇時點並非快到更新時點之前之情形時，不選擇第2逆轉換函數f^{-1}而選擇第1逆轉換函數f^{-1}，於選擇時點為快到更新時點之前之情形時，選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}。選擇伺服器40保持選擇時點是否為快到更新時點之前之判定結果。該判定結果亦可

與自使用者PC30接收到之第1Salt建立關聯並予以保持。逆轉換函數選擇部402於選擇時點並非快到更新時點之前之情形時，僅進行選擇第1逆轉換函數f^{-1}之處理。逆轉換函數選擇部402於選擇時點為快到更新時點之前之情形時，與變化例1同樣，選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}。

【0158】

逆轉換函數選擇部208於選擇時點並非快到更新時點之前之情形時，選擇第1逆轉換函數f^{-1}，於選擇時點為快到更新時點之前之情形時，選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}中之任一者。逆轉換函數選擇部208於選擇時點並非快到更新時點之前之情形時，因自選擇伺服器40僅接收顯示第1逆轉換函數f^{-1}之資訊，故只要直接選擇第1逆轉換函數f^{-1}即可。逆轉換函數選擇部208於選擇時點為快到更新時點之前之情形時，與變化例1同樣，只要選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}中之任一者即可。

【0159】

根據變化例2，選擇伺服器40於選擇時點並非快到更新時點之前之情形時，不選擇第2逆轉換函數f^{-1}而選擇第1逆轉換函數f^{-1}，於選擇時點為快到更新時點之前之情形時，選擇第1逆轉換函數f^{-1}及第2逆轉換函數f^{-1}。藉此，可將無需變化例1般之處理時之處理簡化。其結果，可減輕認證伺服器20、使用者PC30、及選擇伺服器40之處理負荷。

【0160】

[4-3.變化例3]

例如，如第2實施形態及第3實施形態般，於基於第1Salt之一部分選擇轉換函數f及逆轉換函數f^{-1}之情形時，該一部分可動態改變。即，於圖8及圖11之例中，說明基於第1Salt之後1碼選擇轉換函數f及逆轉換函數f^{-1}

之情形，但亦可以基於第1Salt之前1碼或第2碼選擇轉換函數f及逆轉換函數f^{-1}之方式，動態改變。

【0161】

轉換函數選擇部306可基於特定之決定方法，決定轉換函數f之選擇所利用之一部分，基於該決定之一部分，選擇複數個轉換方法中之任一者。該決定方法係決定第1Salt中之哪一部分由轉換函數f及逆轉換函數f^{-1}之選擇利用之方法。該決定方法只要為預定之方法即可，可為隨機選擇第1Salt中之特定之碼之方法，亦可為管理者指定之方法。

【0162】

於變化例3中，轉換函數選擇部306基於特定之決定方法，決定第1Salt中之任1碼作為轉換函數f之選擇所利用之一部分。該1碼之值、與轉換函數f之關係可與圖8及圖11同樣。轉換函數選擇部306於第1Salt中，基於根據特定之決定方法決定之1碼之值，選擇轉換函數f。例如，若該1碼之值為「1」，則選擇轉換函數f1。若該1碼之值為「7」，則選擇轉換函數f7。

【0163】

認證伺服器20之逆轉換函數選擇部208基於特定之決定方法，決定逆轉換函數f^{-1}之選擇所利用之一部分，基於該決定之一部分，選擇複數個逆轉換函數f^{-1}中之任一者。該決定方法與上述之決定方法相同。逆轉換函數f^{-1}之選擇方法亦與轉換函數f之選擇方法同樣。

【0164】

根據變化例3，轉換函數f及逆轉換函數f^{-1}之選擇所利用之部分動態改變。藉此，因第三者不易特定轉換函數f及逆轉換函數f^{-1}之選擇之組

成，故通信之安全性進而提高。

【0165】

[4-4.變化例4]

例如，於使用者登錄之前，由於有惡意之第三者之跨網站指令碼攻擊等，盜取使用者PC30內之TUID、轉換函數f、對Salt伺服器10之訪問方法(例如對特定之IP(Internet Protocol)位址發送createSaltPair()之指令取得Salt之流程)、及使用者之臉部照片。於該情形時，即使於使用者每次登錄時更新TUID，亦有因第三者獲取訪問Salt伺服器10之一連串流程、與認證所需之資訊，故可冒充之虞。

【0166】

因此，於使用者於認證伺服器20登錄臉部照片等資訊、或利用使用者ID及密碼等以安全之方法登錄之情形時，使用者PC30亦可產生基於自身相關之複數個資訊之哈希值並發送至認證伺服器20。該哈希值與使用者ID建立關聯並存儲於使用者資料庫DB2。於使用者執行利用TUID之認證登錄之情形時，使用者PC30轉換TUID，對認證伺服器20發送轉換後之TUID、與基於使用者PC30相關之複數個資訊之哈希值。如第1實施形態等說明般，發送部304亦發送使用者之臉部照片。

【0167】

認證伺服器20將轉換後之TUID進行逆轉換取得TUID，基於該取得之TUID、與哈希值，執行認證處理。因第1實施形態等說明之通信系統S除TUID認證外，亦兼用臉部認證，故認證伺服器20基於TUID、臉部之特徵量、及哈希值，執行認證處理。因此，變化例4之認證處理成為三要素認證。利用TUID與臉部之特徵量之認證如第1實施形態等所說明般。認證

伺服器20判定自使用者PC30接收到之哈希值、與與使用者之使用者ID建立關聯並存儲於使用者資料庫DB2之哈希值是否一致。於該等一致之情形時，利用哈希值之認證成功。

【0168】

另，作為用於產生哈希值之複數個資訊，可組合任意之資訊。例如，使用者PC30可基於使用者PC30之種類、作業系統之種類、瀏覽器之種類之複數個資訊，產生哈希值。此外例如，亦可基於使用者PC30之串列編號、SIM(Subscriber Identity Module：用戶身份模組)卡之編號、或通信卡之MAC(Media Access Control：媒體存取控制)位址之其他資訊，產生哈希值。用於產生哈希值之哈希函數自身可利用各種哈希函數。哈希值並非記憶於使用者PC30，而於每次認證時產生。

【0169】

根據變化例4之通信系統S，藉由利用哈希值之認證，安全性提高。例如，即使有惡意之第三者非法獲取使用者PC30內之TUID等，亦因無法特定至哈希值之可能性較高，故安全性提高。

【0170】

[4-5.變化例5]

例如，通信系統S可應用於執行認證處理之場景以外之其他場景。作為其他場景，於發送電子郵件之場景、上傳或下載檔案之場景、進行SNS(Social Networking Services：社交網路服務)之投稿之場景、使瀏覽器顯示某種頁面之場景、或使用者上傳或下載個人資訊之場景之其他畫面亦可應用通信系統S。

【0171】

例如，若於發送電子郵件之場景應用通信系統S，則第1裝置為電子郵件之發送側之電腦，第2裝置為電子郵件之接收側之電腦。原資料為電子郵件之資料。於原資料，包含電子郵件之正文。於對電子郵件附加附加檔案之情形時，於原資料包含附加檔案。第1裝置基於第2Salt，對電子郵件即原資料進行轉換，產生轉換資料。轉換資料為轉換後之電子郵件。第1裝置對第2裝置發送第1Salt、與轉換後之電子郵件即轉換資料。第2裝置若接收第1Salt及轉換資料，則基於第1Salt取得第2Salt，基於該取得之第2Salt進行轉換資料之逆轉換，取得原資料即電子郵件。第1Salt及第2Salt之取得方法如第1實施形態～第3實施形態及變化例1～4所說明般。

【0172】

例如，若於上傳檔案之場景應用通信系統S，則第1裝置為上傳檔案之使用者之電腦，第2裝置為接收檔案之伺服器。原資料為上傳對象之檔案。第1裝置基於第1Salt，對上傳對象之檔案即原資料進行轉換，產生轉換資料。轉換資料係轉換後之檔案。第1裝置對第2裝置發送第1Salt、與轉換後之檔案即轉換資料。第2裝置若接收轉換資料，則基於第1Salt取得第2Salt，基於該取得之第2Salt進行逆轉換，取得原資料即檔案。第1Salt及第2Salt之取得方法如第1實施形態～第3實施形態及變化例1～4所說明般。

【0173】

於其他場景應用通信系統S之情形亦同樣，第1裝置只要基於複數個Salt，轉換原資料並對第2裝置發送轉換資料即可。第2裝置只要基於複數個Salt，將轉換資料進行逆轉換取得原資料即可。根據變化例5之通信系統S，各種場景之通信之安全性提高。

【0174】

[4-6.其他變化例]

例如，可組合第1實施形態～第3實施形態。亦可組合上述變化例。

【0175】

例如，作為由Salt伺服器10實現者說明之功能可由認證伺服器20或使用者PC30實現。於該情形時，通信系統S可不包含Salt伺服器10。例如，於通信系統S包含複數個伺服器電腦之情形時，可由複數個伺服器電腦分擔功能。又例如，作為由資料記憶部100、200記憶者說明之資料亦可藉由Salt伺服器10或認證伺服器20以外之電腦記憶。

【符號說明】

【0176】

10:Salt伺服器

11:控制部

12:記憶部

13:通信部

20:認證伺服器

21:控制部

22:記憶部

23:通信部

30:使用者PC

31:控制部

32:記憶部

33:通信部

34:操作部

35:顯示部

36:攝影部

40:選擇伺服器

41:控制部

42:記憶部

43:通信部

100:資料記憶部

101:Salt產生部

102:接收部

103:發送部

104:第1刪除部

105:第2刪除部

200:資料記憶部

201:接收部

202:Salt請求部

203:Salt取得部

204:逆轉換部

205:處理執行部

206:TUID產生部

207:發送部

208:逆轉換函數選擇部

209:逆轉換函數請求部

300:資料記憶部

301:Salt請求部

302:Salt取得部

303:轉換部

304:發送部

305:接收部

306:轉換函數選擇部

307:轉換函數請求部

400:資料記憶部

401:轉換函數選擇部

402:逆轉換函數選擇部

403:更新部

DB1:Salt資料庫

DB2:使用者資料庫

DB3:函數資料庫

N:網路

S:通信系統

S1～S22:步驟

【發明申請專利範圍】

【請求項1】

一種通信系統，其係包含第1裝置、第2裝置及選擇裝置者，且

包含產生部，其基於來自上述第1裝置之請求，產生複數個資訊，該複數個資訊包含：用於選擇原資料之轉換方法及逆轉換方法之第1資訊；及用於轉換及逆轉換之第2資訊；

上述第1裝置包含：

資訊取得部，其取得上述第1資訊及上述第2資訊；及

轉換方法請求部，其基於上述第1資訊，對上述選擇裝置請求原資料之轉換方法之選擇；

上述選擇裝置包含：轉換方法選擇部，其基於來自上述第1裝置之請求，選擇複數個上述轉換方法中之任一者；

上述第1裝置包含：

轉換方法選擇部，其基於上述選擇裝置之選擇結果，選擇上述轉換方法；

轉換部，其基於藉由上述第1裝置之上述轉換方法選擇部選擇之上述轉換方法及上述第2資訊，轉換上述原資料產生轉換資料；及

發送部，其對上述第2裝置，發送上述第1資訊及上述轉換資料；

上述第2裝置包含：

接收部，其自上述第1裝置，接收上述第1資訊及上述轉換資料；

資訊取得部，其基於上述第1資訊，取得上述第2資訊；及

逆轉換方法請求部，其基於上述第1資訊，對上述選擇裝置請求上述原資料之逆轉換方法之選擇；

上述選擇裝置包含：逆轉換方法選擇部，其基於來自上述第2裝置之請求，選擇複數個上述逆轉換方法中之任一者；

上述第2裝置包含：

逆轉換方法選擇部，其基於上述選擇裝置之選擇結果，選擇上述逆轉換方法，

逆轉換部，其基於上述第2資訊及藉由上述第2裝置之上述逆轉換方法選擇部選擇之上述逆轉換方法，逆轉換上述轉換資料取得上述原資料。

【請求項2】

如請求項1之通信系統，其中

上述選擇裝置包含將上述第1資訊相關之選擇條件、與上述複數個轉換方法及上述複數個逆轉換方法之各者之關聯更新之更新部。

【請求項3】

如請求項2之通信系統，其中

上述更新部於預定之更新時點來臨之情形時，更新上述關聯，

上述發送部對上述第2裝置，進而發送選擇了上述轉換方法之選擇時點相關之時點資訊，

上述選擇裝置之上述逆轉換方法選擇部，於更新上述關聯緊接之後立即受理來自上述第2裝置之請求之情形時，基於更新前之關聯，選擇第1逆轉換方法，且基於更新後之關聯，選擇第2逆轉換方法，

上述第2裝置之上述逆轉換方法選擇部，基於上述時點資訊，選擇上述第1逆轉換方法及上述第2逆轉換方法中之任一者。

【請求項4】

如請求項3之通信系統，其中

上述第1裝置，於上述選擇時點並非快到上述更新時點之前之情形時，不對上述第2裝置發送上述時點資訊，於上述選擇時點為快到上述更新時點之前之情形時，對上述第2裝置發送上述時點資訊，

上述選擇裝置之上述逆轉換方法選擇部，於上述選擇時點並非快到上述更新時點之前之情形時，不選擇上述第2逆轉換方法而選擇上述第1逆轉換方法，於上述選擇時點為快到上述更新時點之前之情形時，選擇上述第1逆轉換方法及上述第2逆轉換方法，

上述第2裝置之上述逆轉換方法選擇部，於上述選擇時點並非快到上述更新時點之前之情形時，選擇上述第1逆轉換方法，於上述選擇時點為快到上述更新時點之前之情形時，選擇上述第1逆轉換方法及上述第2逆轉換方法中之任一者，

上述快到上述更新時點之前係：自上述選擇時點至上述更新時點之時間未達閾值。

【請求項5】

一種通信系統，其係包含第1裝置及第2裝置者，且

包含產生部，其基於來自上述第1裝置之請求產生複數個資訊，該複數個資訊包含：用於選擇原資料之轉換方法及逆轉換方法之第1資訊；及用於轉換及逆轉換之第2資訊；

上述第1裝置包含：

資訊取得部，其取得上述第1資訊及上述第2資訊；

轉換方法選擇部，其基於一部分，選擇複數個上述轉換方法中之任一者，該一部分係：於上述第1資訊中，隨機決定為由上述轉換方法之選擇所利用之一部分；

轉換部，其基於藉由上述轉換方法選擇部選擇之上述轉換方法及上述第2資訊，轉換上述原資料產生轉換資料；及

發送部，其對上述第2裝置，發送上述第1資訊及上述轉換資料；

上述第2裝置包含：

接收部，其自上述第1裝置，接收上述第1資訊及上述轉換資料；

資訊取得部，其基於上述第1資訊，取得上述第2資訊；

逆轉換方法選擇部，其基於隨機決定之上述一部分，選擇複數個上述逆轉換方法中之任一者；及

逆轉換部，其基於藉由上述逆轉換方法選擇部選擇之上述逆轉換方法及上述第2資訊，逆轉換上述轉換資料取得上述原資料。

【請求項6】

如請求項5之通信系統，其中

上述轉換方法選擇部係不對其他裝置請求上述轉換方法之選擇，而基於上述第1資訊，選擇複數個上述轉換方法中之任一者，

上述逆轉換方法選擇部係不對其他裝置請求上述逆轉換方法之選擇，而基於上述第1資訊，選擇上述複數個逆轉換方法中之任一者。

【請求項7】

如請求項1至6中任一項之通信系統，其中

上述通信系統包含管理裝置，

上述管理裝置包含上述產生部，管理上述第1資訊及上述第2資訊，

上述第1裝置包含對上述管理裝置，請求上述第1資訊及上述第2資訊之資訊請求部，

上述管理裝置之上述產生部基於來自上述第1裝置之請求，產生上述

第1資訊及上述第2資訊，

上述第2裝置包含基於上述第1資訊，對上述管理裝置請求上述第2資訊之資訊請求部，

上述管理裝置基於來自上述第2裝置之請求，對上述第2裝置發送上述第2資訊。

【請求項8】

如請求項7之通信系統，其中

上述第1裝置之上述資訊請求部對上述管理裝置，發送請求，該請求不包含上述第1資訊及上述第2資訊之取得規則相關之資訊。

【請求項9】

如請求項1至6中任一項之通信系統，其中

上述原資料係上述第1裝置之使用者相關之認證資料，

上述第1裝置轉換上述認證資料，對上述第2裝置發送上述轉換資料，

上述第2裝置逆轉換上述轉換資料取得上述認證資料，基於該取得之認證資料，執行上述使用者相關之認證處理，產生新的上述認證資料。

【請求項10】

如請求項1至6中任一項之通信系統，其中

上述原資料係上述第1裝置之使用者相關之認證資料，

上述第1裝置轉換上述認證資料，對上述第2裝置發送上述轉換資料、及基於上述第1裝置相關之複數個資訊之哈希值，

上述第2裝置逆轉換上述轉換資料取得上述認證資料，基於該取得之認證資料、及上述哈希值，執行上述使用者相關之認證處理。

【請求項11】

如請求項10之通信系統，其中

上述第2裝置基於自上述第1裝置接收之上述哈希值及預先存儲於資料庫之哈希值，執行上述認證處理。

【請求項12】

如請求項1至6中任一項之通信系統，其中

上述通信系統進而包含於產生上述複數個資訊之後，預定之刪除時點來臨之情形時，刪除上述複數個資訊之第1刪除部。

【請求項13】

如請求項1至6中任一項之通信系統，其中

上述通信系統進而包含基於來自上述第2裝置之請求，刪除上述複數個資訊之第2刪除部。

【請求項14】

一種通信方法，其係第1裝置、第2裝置及選擇裝置之間之通信方法，且基於來自上述第1裝置之請求，產生複數個資訊，該複數個資訊包含：用於選擇原資料之轉換方法及逆轉換方法之第1資訊；及用於轉換及逆轉換之第2資訊，

上述第1裝置

取得上述第1資訊及上述第2資訊，

基於上述第1資訊，對上述選擇裝置請求原資料之轉換方法之選擇；

上述選擇裝置基於來自上述第1裝置之請求，選擇複數個上述轉換方法中之任一者；

上述第1裝置

基於上述選擇裝置之選擇結果，選擇上述轉換方法，

基於藉由上述第1裝置選擇之上述轉換方法及上述第2資訊，轉換上述原資料產生轉換資料，

對上述第2裝置，發送上述第1資訊及上述轉換資料；

上述第2裝置

自上述第1裝置，接收上述第1資訊及上述轉換資料，

基於上述第1資訊，取得上述第2資訊，

基於上述第1資訊，對上述選擇裝置請求上述原資料之逆轉換方法之選擇；

上述選擇裝置基於來自上述第2裝置之請求，選擇複數個上述逆轉換方法中之任一者；

上述第2裝置

基於上述選擇裝置之選擇結果，選擇上述逆轉換方法，

基於上述第2資訊及藉由上述第2裝置選擇之上述逆轉換方法，逆轉換上述轉換資料取得上述原資料。

【請求項15】

一種程式產品，其用於使電腦作為第1裝置、第2裝置、選擇裝置及產生部發揮功能，該第1裝置可與該第2裝置及該選擇裝置進行通信，

上述產生部基於來自上述第1裝置之請求，產生複數個資訊，該複數個資訊包含：用於選擇原資料之轉換方法及逆轉換方法之第1資訊；及用於轉換及逆轉換之第2資訊，

上述第1裝置具有：

資訊取得部，其取得上述複數個資訊，該複數個資訊包含：上述第1

資訊及上述第2資訊；

轉換方法請求部，其基於上述第1資訊，對上述選擇裝置請求原資料之轉換方法之選擇；

轉換方法選擇部，其基於上述選擇裝置之選擇結果，選擇上述轉換方法；

轉換部，其基於藉由上述第1裝置之上述轉換方法選擇部選擇之上述轉換方法及上述第2資訊，轉換上述原資料而產生轉換資料；及

發送部，其對上述第2裝置，發送上述第1資訊及上述轉換資料；且

上述選擇裝置包含：轉換方法選擇部，其基於來自上述第1裝置之請求，選擇複數個上述轉換方法中之任一者。

【請求項16】

一種程式產品，其用於使電腦作為可與第1裝置及選擇裝置進行通信之第2裝置發揮功能，

上述第2裝置具有：

接收部，其自上述第1裝置，接收基於複數個資訊對原資料轉換之轉換資料及第1資訊，該複數個資訊包含：基於來自上述第1裝置之請求而產生之用於選擇原資料之轉換方法及逆轉換方法之上述第1資訊及用於轉換及逆轉換之第2資訊；

資訊取得部，其基於上述第1資訊，取得上述第2資訊；

逆轉換方法請求部，其基於上述第1資訊，對上述選擇裝置請求上述原資料之逆轉換方法之選擇；

逆轉換方法選擇部，其基於上述選擇裝置之選擇結果，選擇上述逆轉換方法；及

逆轉換部，其基於上述第2資訊及藉由上述第2裝置之上述逆轉換方法選擇部選擇之上述逆轉換方法，逆轉換上述轉換資料而取得上述原資料；且

上述選擇裝置包含：逆轉換方法選擇部，其基於來自上述第2裝置之請求，選擇複數個上述逆轉換方法中之任一者。

【請求項17】

一種通信方法，其係第1裝置及第2裝置之間之通信方法，且基於來自上述第1裝置之請求，產生複數個資訊，該複數個資訊包含：用於選擇原資料之轉換方法及逆轉換方法之第1資訊；及用於轉換及逆轉換之第2資訊，

上述第1裝置

取得上述第1資訊及上述第2資訊，

基於一部分，選擇複數個上述轉換方法中之任一者，該一部分係：於上述第1資訊中，隨機決定為由上述轉換方法之選擇所利用之一部分，

基於上述選擇之轉換方法及上述第2資訊，轉換上述原資料產生轉換資料，

對上述第2裝置，發送上述第1資訊及上述轉換資料；

上述第2裝置

自上述第1裝置，接收上述第1資訊及上述轉換資料，

基於上述第1資訊，取得上述第2資訊，

基於隨機決定之上述一部分，選擇複數個上述逆轉換方法中之任一者，

基於上述選擇之逆轉換方法及上述第2資訊，逆轉換上述轉換資料取

得上述原資料。

【請求項18】

一種程式產品，其用於使電腦作為可與第1裝置進行通信之第2裝置發揮功能，

上述第2裝置具有：

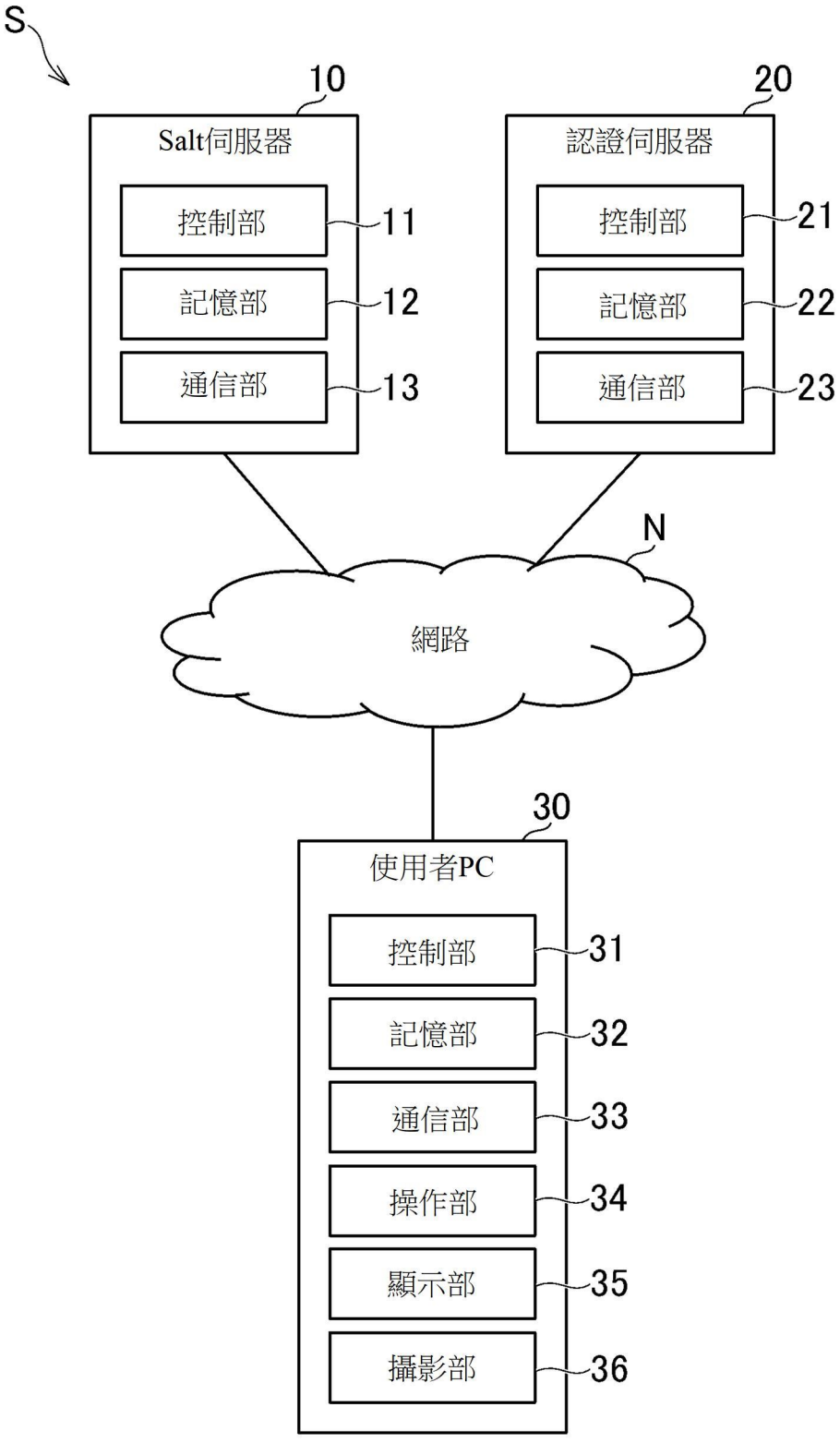
接收部，其自上述第1裝置，接收基於複數個資訊對原資料轉換之轉換資料及第1資訊，該複數個資訊包含：基於來自上述第1裝置之請求而產生之用於選擇原資料之轉換方法及逆轉換方法之上述第1資訊及用於轉換及逆轉換之第2資訊；

資訊取得部，其基於上述第1資訊，取得上述第2資訊；

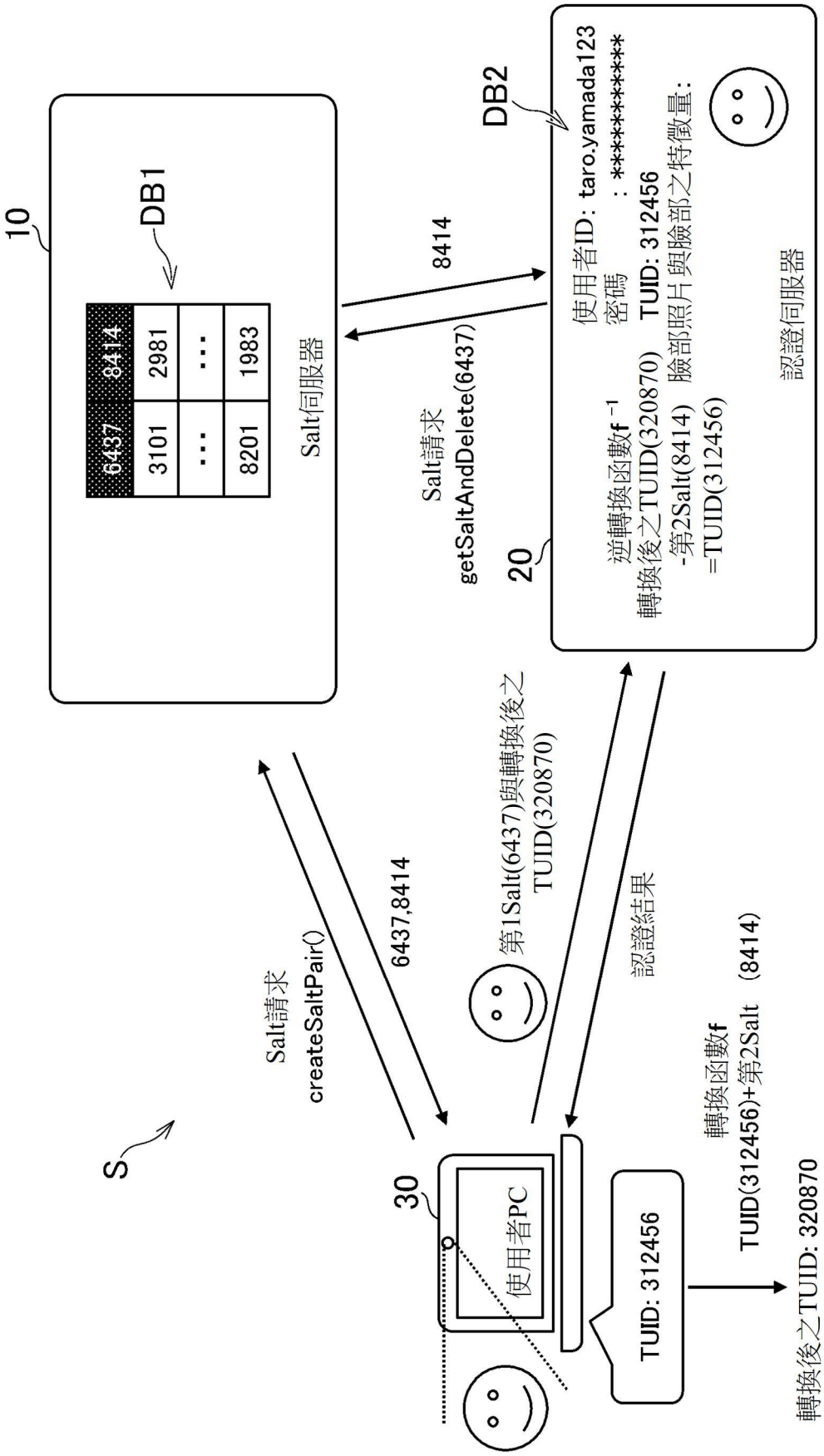
逆轉換方法選擇部，其基於於上述第1資訊中，隨機決定之一部分，選擇複數個上述逆轉換方法中之任一者；及

逆轉換部，其基於藉由上述逆轉換方法選擇部選擇之上述逆轉換方法及上述第2資訊，逆轉換上述轉換資料取得上述原資料。

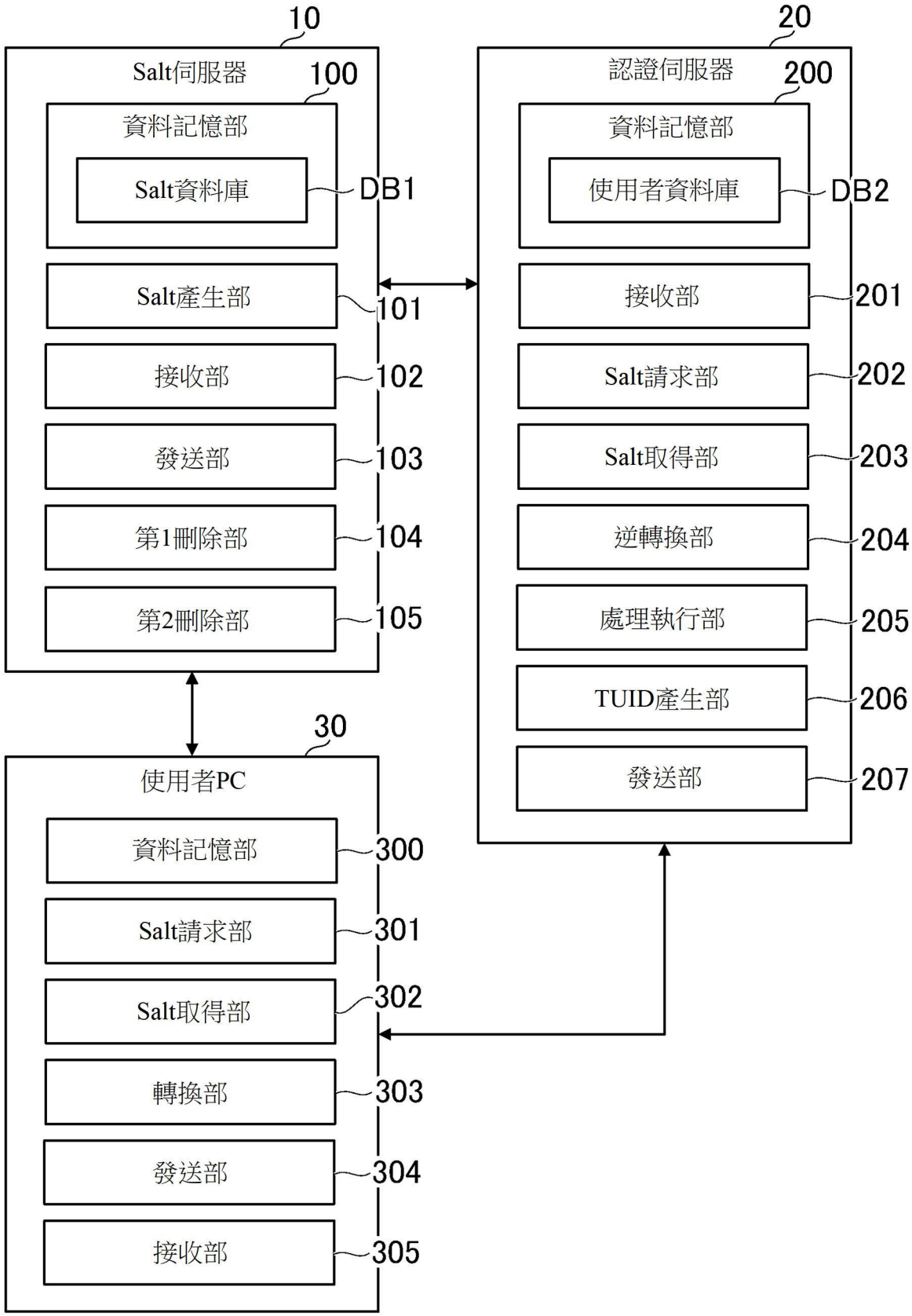
【發明圖式】


S
10
Salt伺服器
控制部
11
記憶部
12
通信部
13
20
認證伺服器
控制部
21
記憶部
22
通信部
23
N
網路
30
使用者PC
控制部
31
記憶部
32
通信部
33
操作部
34
顯示部
35
攝影部
36

【圖1】


10
DB1
6437
8414
3101
2981
...
...
8201
1983
Salt伺服器
8414
Salt請求
getSaltAndDelete(6437)
DB2
20
使用者ID: taro.yamada123
密碼 : **********
逆轉換函數f -1
轉換後之TUID(320870) TUID: 312456
-第2Salt(8414) 臉部照片與臉部之特徵量:
=TUID(312456)
認證伺服器
S
Salt請求
createSaltPair()
6437,8414
第1Salt(6437)與轉換後之
TUID(320870)
認證結果
30
使用者PC
TUID: 312456
轉換函數f
TUID(312456)+第2Salt (8414)
轉換後之TUID: 320870

【圖2】

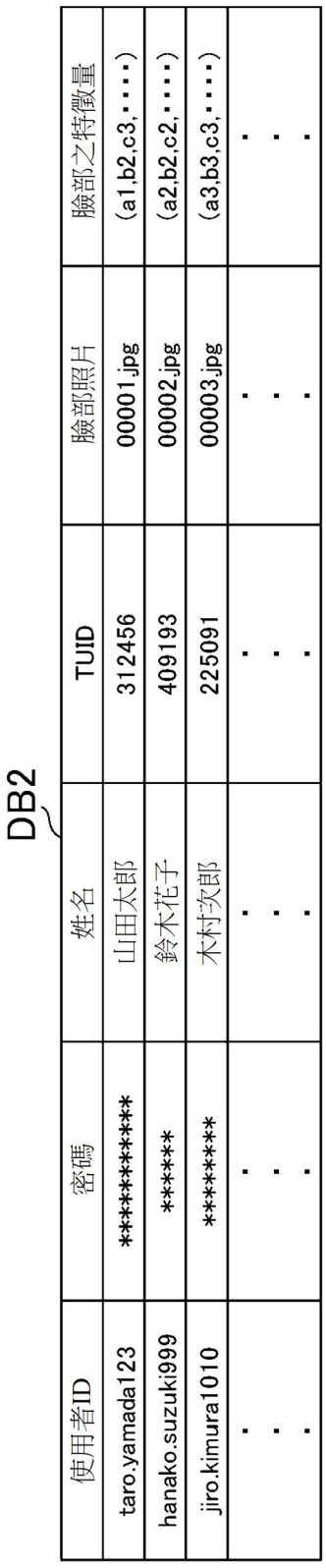

10
Salt伺服器
100
資料記憶部
Salt資料庫
DB1
Salt產生部
101
接收部
102
發送部
103
第1刪除部
104
第2刪除部
105
20
認證伺服器
200
資料記憶部
使用者資料庫
DB2
接收部
201
Salt請求部
202
Salt取得部
203
逆轉換部
204
處理執行部
205
TUID產生部
206
發送部
207
30
使用者PC
資料記憶部
300
Salt請求部
301
Salt取得部
302
轉換部
303
發送部
304
接收部
305

【圖3】

DB1

第1Salt	第2Salt
6437	8414
3101	2981
⋮	⋮
8201	1983

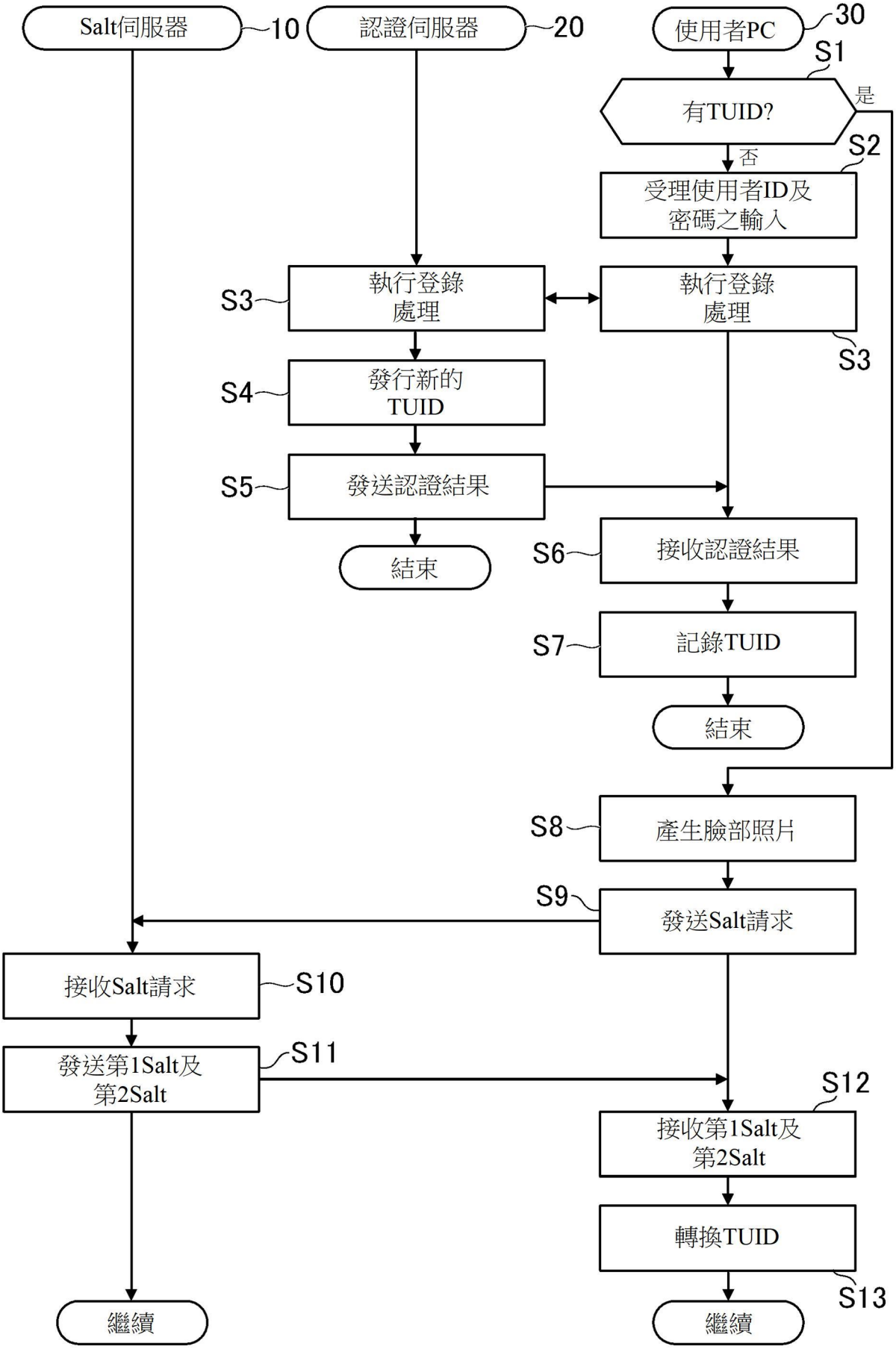
【圖4】



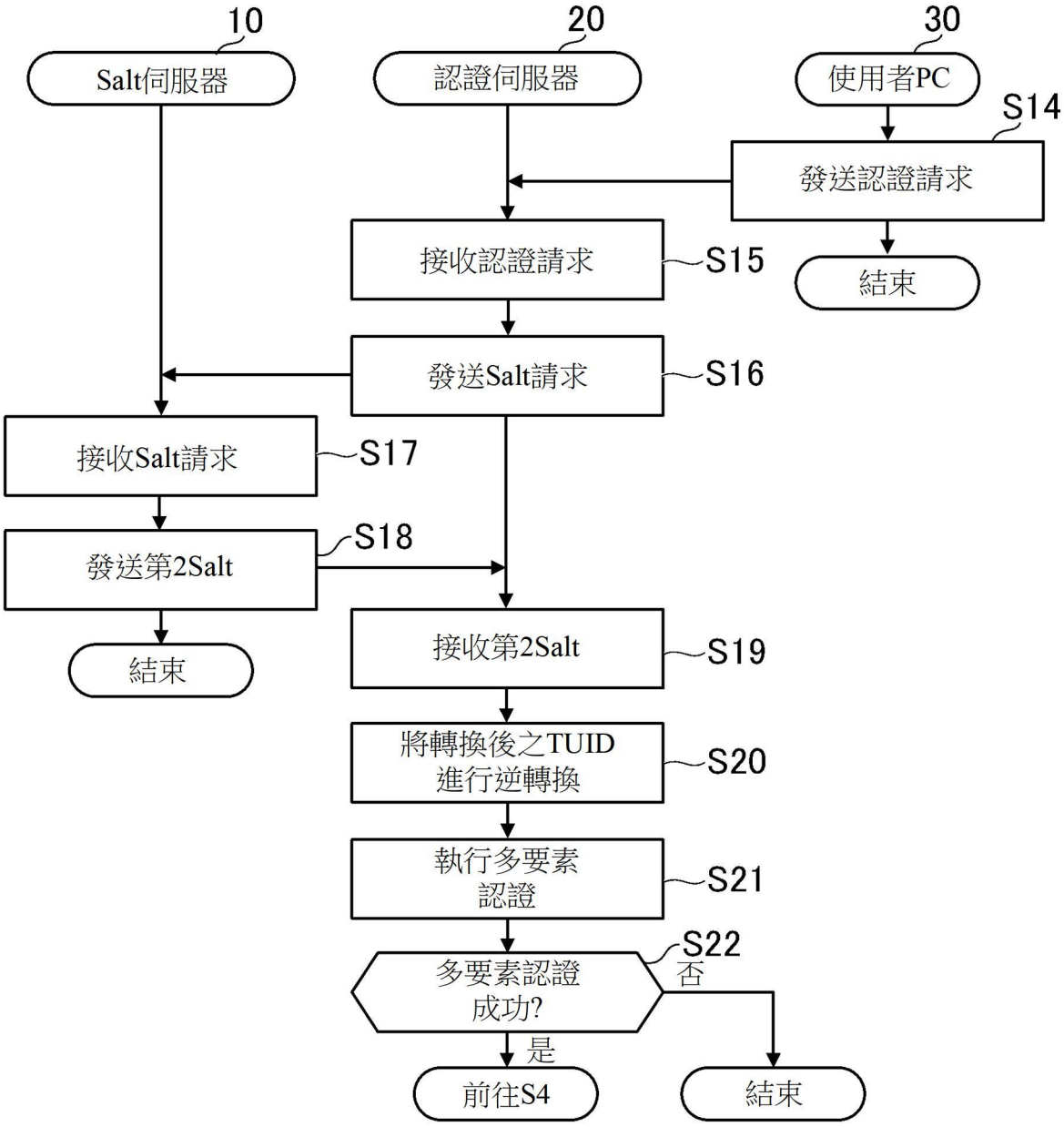
DB2

使用者ID	密碼	姓名	TUID	臉部照片	臉部之特徵量
taro.yamada123	**********	山田太郎	312456	00001.jpg	(a1,b2,c3,‧‧‧‧)
hanako.suzuki999	*******	鈴木花子	409193	00002.jpg	(a2,b2,c2,‧‧‧‧)
jiro.kimura1010	********	木村次郎	225091	00003.jpg	(a3,b3,c3,‧‧‧‧)
‧	‧	‧	‧	‧	‧
‧	‧	‧	‧	‧	‧
‧	‧	‧	‧	‧	‧

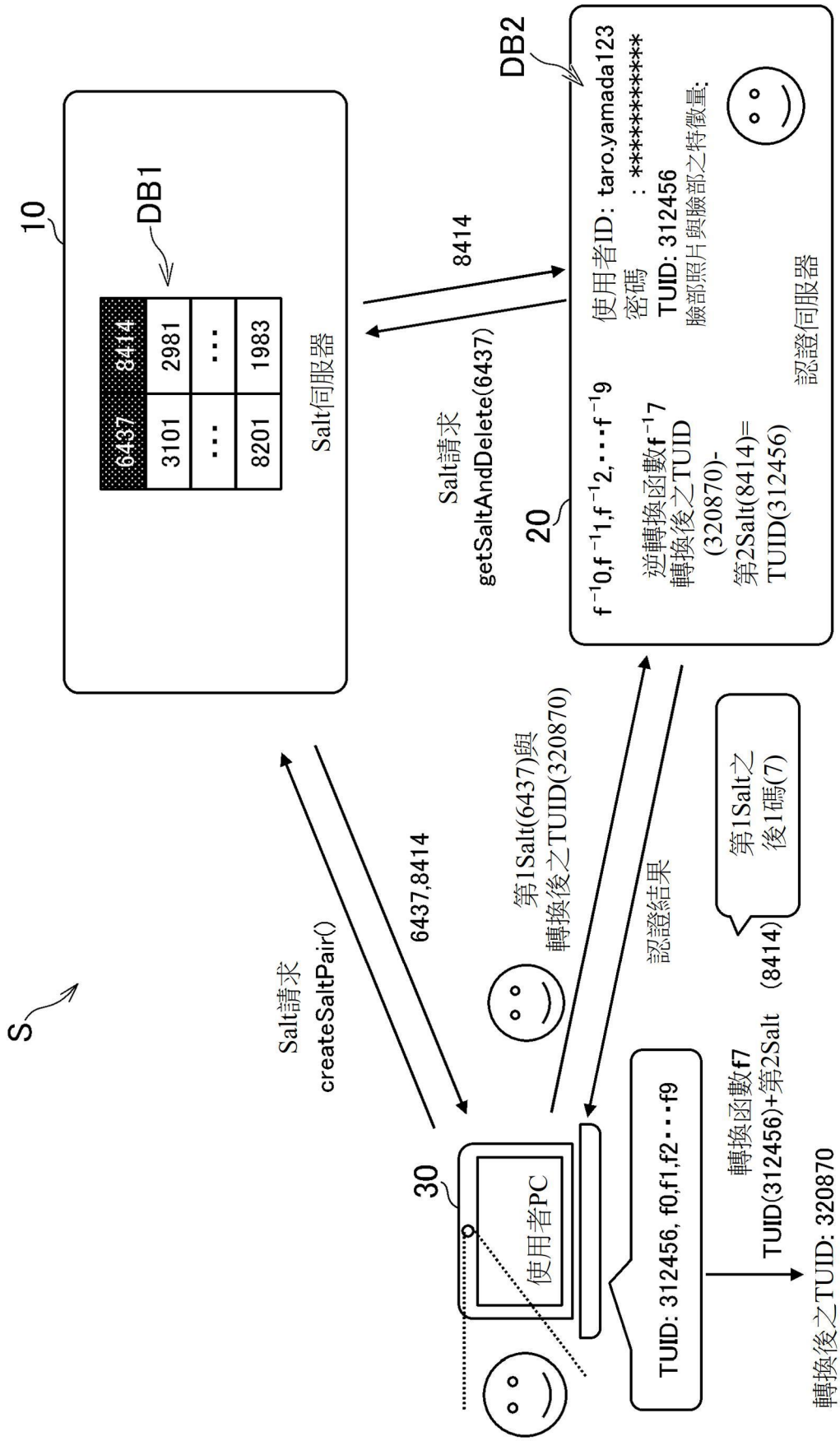
【圖5】


Salt伺服器
10
認證伺服器
20
使用者PC
30
S1
有TUID?
是
否
S2
受理使用者ID及
密碼之輸入
S3
執行登錄
處理
執行登錄
處理
S3
S4
發行新的
TUID
S5
發送認證結果
結束
S6
接收認證結果
S7
記錄TUID
結束
S8
產生臉部照片
S9
發送Salt請求
接收Salt請求
S10
發送第1Salt及
第2Salt
S11
S12
接收第1Salt及
第2Salt
轉換TUID
S13
繼續
繼續

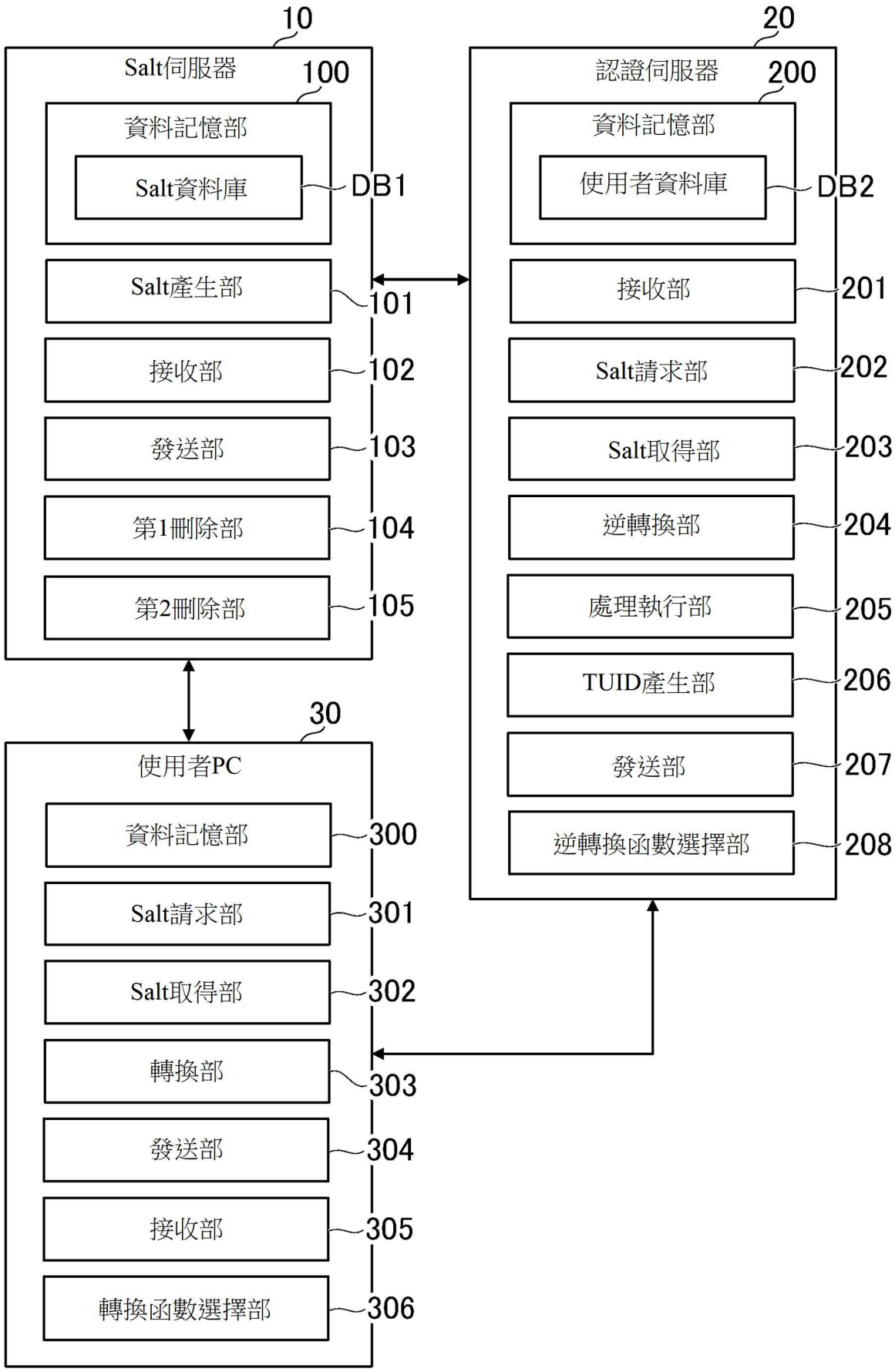
【圖6】


10
Salt伺服器
20
認證伺服器
30
使用者PC
S14
發送認證請求
結束
接收認證請求
S15
發送Salt請求
S16
接收Salt請求
S17
發送第2Salt
S18
結束
接收第2Salt
S19
將轉換後之TUID
進行逆轉換
S20
執行多要素
認證
S21
S22
多要素認證
成功?
否
是
前往S4
結束

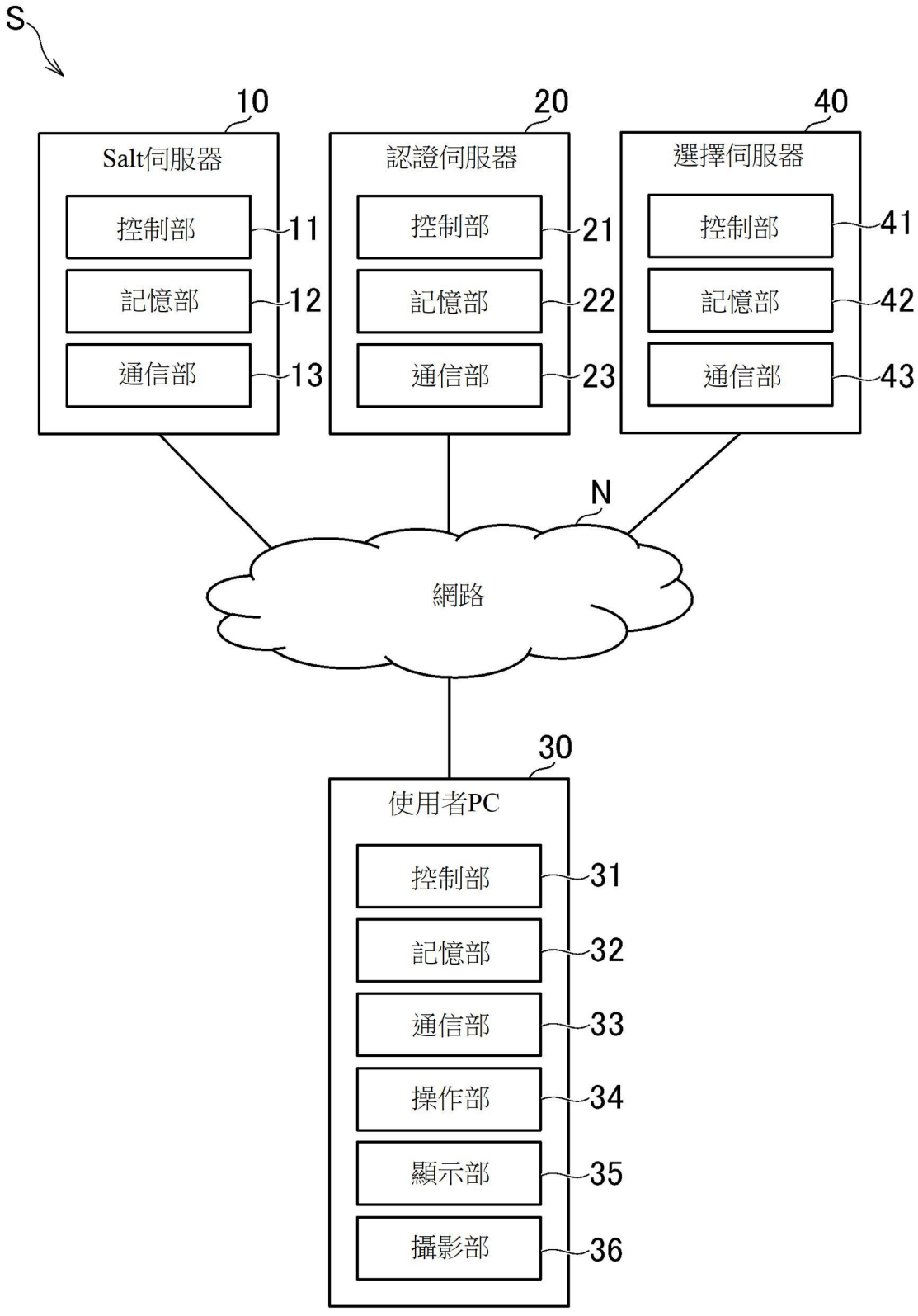
【圖7】


S
10
DB1
6437
8414
3101
2981
...
...
8201
1983
Salt伺服器
8414
Salt請求
getSaltAndDelete(6437)
20
DB2
f⁻¹0,f⁻¹1,f⁻¹2,･･･f⁻¹9
逆轉換函數f⁻¹7
轉換後之TUID
(320870)-
第2Salt(8414)=
TUID(312456)
使用者ID: taro.yamada123
密碼 : **********
TUID: 312456
臉部照片與臉部之特徵量:
認證伺服器
Salt請求
createSaltPair()
6437,8414
第1Salt(6437)與
轉換後之TUID(320870)
認證結果
第1Salt之
後1碼(7)
(8414)
30
使用者PC
TUID: 312456, f0,f1,f2･･･f9
轉換函數f7
TUID(312456)+第2Salt
轉換後之TUID: 320870

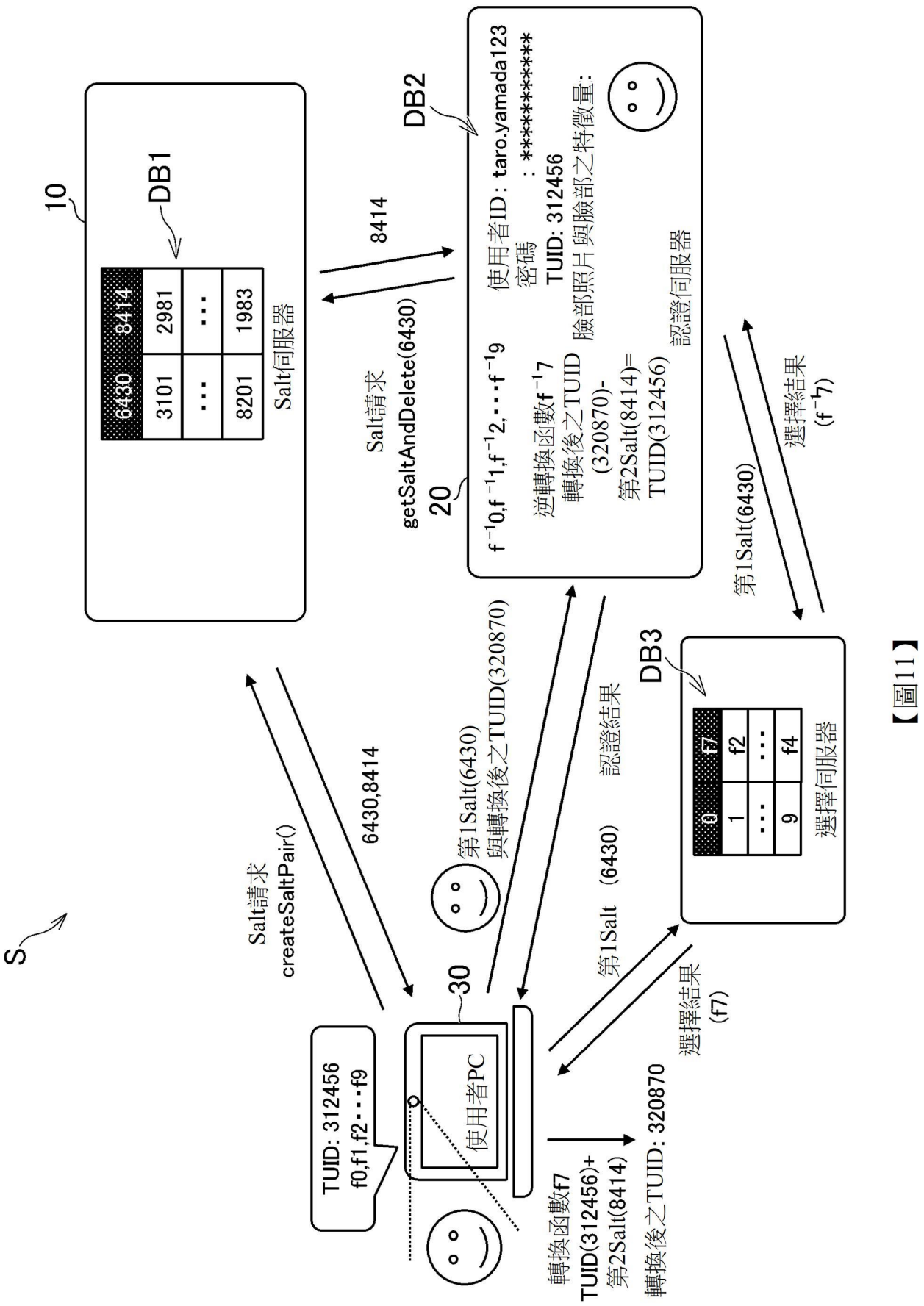
【圖8】


10
Salt伺服器
100
資料記憶部
Salt資料庫
DB1
Salt產生部
101
接收部
102
發送部
103
第1刪除部
104
第2刪除部
105
20
認證伺服器
200
資料記憶部
使用者資料庫
DB2
接收部
201
Salt請求部
202
Salt取得部
203
逆轉換部
204
處理執行部
205
TUID產生部
206
發送部
207
逆轉換函數選擇部
208
30
使用者PC
資料記憶部
300
Salt請求部
301
Salt取得部
302
轉換部
303
發送部
304
接收部
305
轉換函數選擇部
306

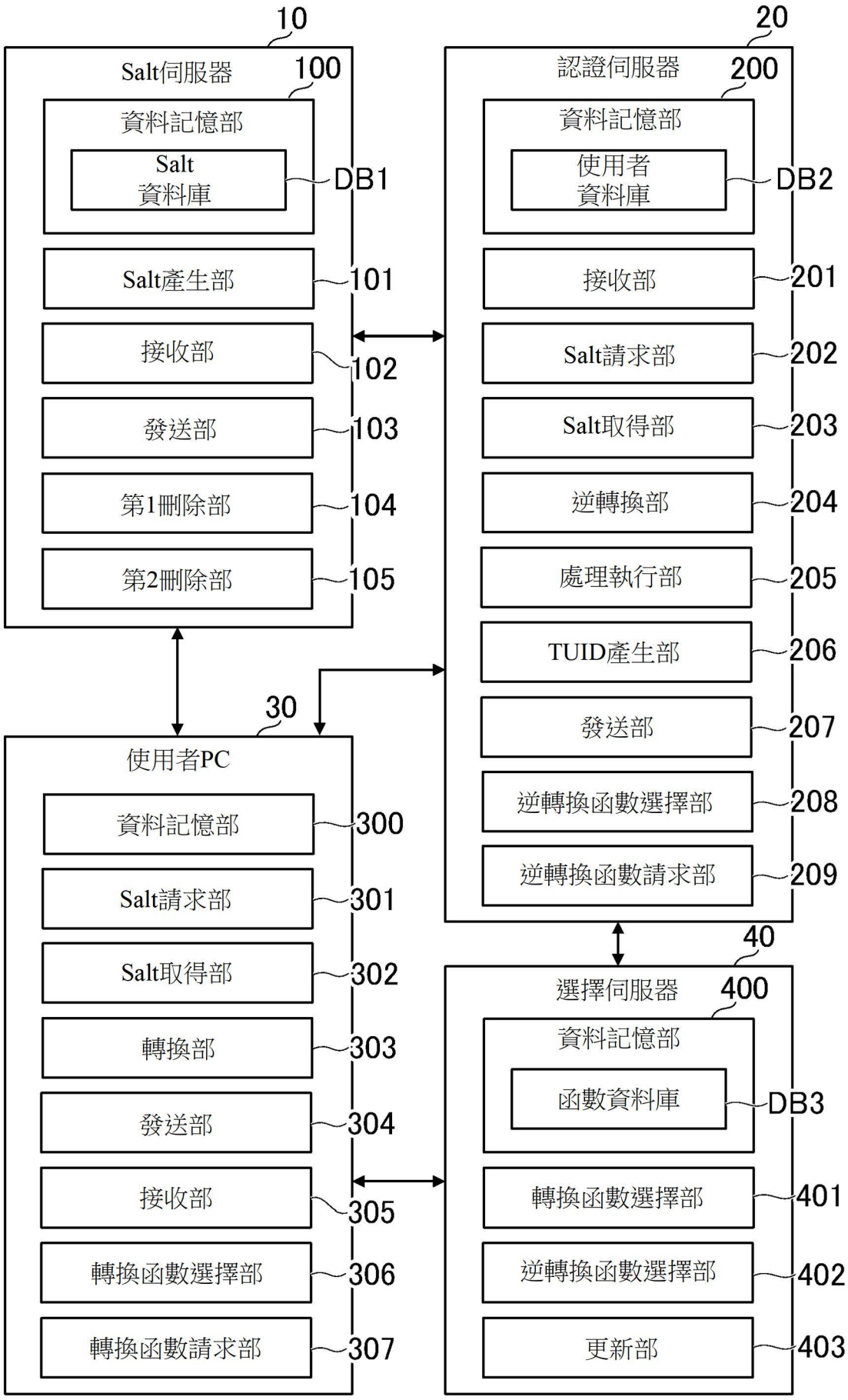
【圖9】


S
10
Salt伺服器
控制部
11
記憶部
12
通信部
13
20
認證伺服器
控制部
21
記憶部
22
通信部
23
40
選擇伺服器
控制部
41
記憶部
42
通信部
43
N
網路
30
使用者PC
控制部
31
記憶部
32
通信部
33
操作部
34
顯示部
35
攝影部
36

【圖10】


S
10
DB1
6430
8414
3101
2981
8201
1983
Salt伺服器
8414
Salt請求
getSaltAndDelete(6430)
20
DB2
使用者ID: taro.yamada123
密碼 : **********
TUID: 312456
臉部照片與臉部之特徵量:
逆轉換函數f⁻¹7
轉換後之TUID
(320870)-
第2Salt(8414)=
TUID(312456)
認證伺服器
Salt請求
createSaltPair()
6430,8414
第1Salt(6430)
與轉換後之TUID(320870)
30
TUID: 312456
f0,f1,f2･･･f9
使用者PC
第1Salt (6430)
認證結果
DB3
0
f7
1
f2
9
f4
選擇伺服器
第1Salt(6430)
選擇結果
(f⁻¹7)
選擇結果
(f7)
轉換函數f7
TUID(312456)+
第2Salt(8414)
轉換後之TUID: 320870

【圖11】


10
Salt伺服器
100
資料記憶部
Salt
資料庫
DB1
Salt產生部
101
接收部
102
發送部
103
第1刪除部
104
第2刪除部
105
20
認證伺服器
200
資料記憶部
使用者
資料庫
DB2
接收部
201
Salt請求部
202
Salt取得部
203
逆轉換部
204
處理執行部
205
TUID產生部
206
發送部
207
逆轉換函數選擇部
208
逆轉換函數請求部
209
30
使用者PC
資料記憶部
300
Salt請求部
301
Salt取得部
302
轉換部
303
發送部
304
接收部
305
轉換函數選擇部
306
轉換函數請求部
307
40
選擇伺服器
400
資料記憶部
函數資料庫
DB3
轉換函數選擇部
401
逆轉換函數選擇部
402
更新部
403

【圖12】